KOMMISSIONENS GENOMFÖRANDEBESLUT (EU) 2021/1773

av den 28 juni 2021

i enlighet med Europaparlamentets och rådets direktiv (EU) 2016/680 om adekvat skydd av personuppgifter i Förenade kungariket

[delgivet med nr C(2021) 4801]

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DETTA BESLUT

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIH ([1]), särskilt artikel 36.3, och

av följande skäl:

1. INLEDNING

(1) I Europaparlamentets och rådets direktiv (EU) 2016/680 fastställs regler för överföring av personuppgifter från behöriga myndigheter i unionen till tredjeländer och internationella organisationer i den mån sådana överföringar omfattas av dess tillämpningsområde. Bestämmelserna om behöriga myndigheters internationella överföring av uppgifter fastställs i kapitel V i direktiv (EU) 2016/680, närmare bestämt i artiklarna 35–40. Flödet av personuppgifter till och från länder utanför Europeiska unionen är avgörande för ett effektivt brottsbekämpningssamarbete men det krävs att skyddsnivån för personuppgifter i Europeiska unionen garanteras och inte undergrävs av sådana överföringar ([2]).

(2) Enligt artikel 36.3 i direktiv (EU) 2016/680 får kommissionen genom en genomförandeakt besluta att ett tredjeland, ett territorium eller en eller flera specificerade sektorer inom ett tredjeland eller en internationell organisation säkerställer en adekvat skyddsnivå. Enligt detta villkor får överföring av personuppgifter till ett tredjeland ske utan ytterligare tillstånd (utom när en annan medlemsstat från vilken uppgifterna erhölls måste ge sitt tillstånd till överföringen) i enlighet med artikel 35.1 och skäl 66 i direktiv (EU) 2016/680.

(3) Enligt artikel 36.2 i direktiv (EU) 2016/680 måste antagandet av ett beslut om adekvat skyddsnivå grundas på en omfattande analys av tredjelandets rättsordning. I sin bedömning måste kommissionen avgöra om det berörda tredjelandet garanterar en skyddsnivå som ”i allt väsentligt är likvärdig” med den som säkerställs inom Europeiska unionen (skäl 67 i direktiv (EU) 2016/680). Den standard mot vilken den ”väsentliga likvärdigheten” bedöms är den som fastställs i EU-lagstiftningen, särskilt direktiv (EU) 2016/680, samt rättspraxis från Europeiska unionens domstol ([3]). Dataskyddsstyrelsens referensram för adekvat skyddsnivå är också av betydelse i detta sammanhang ([4]).

(4) Enligt Europeiska unionens domstol kräver detta inte att en identisk skyddsnivå uppnås ([5]). I synnerhet kan de medel som tredjelandet i fråga har till sitt förfogande för att skydda personuppgifter skilja sig från dem som används i Europeiska unionen förutsatt att de i praktiken visar sig vara effektiva för att säkerställa en adekvat skyddsnivå ([6]). Standarden för en adekvat skyddsnivå kräver därför inte att unionens regler kopieras till punkt och pricka. Det handlar snarare om huruvida det utländska systemet som helhet erbjuder den skyddsnivå som krävs med avseende på innehållet i rätten till personlig integritet och genomförandet, övervakningen och verkställandet av det i praktiken ([7]).

([1]) EUT L 119, 4.5.2016, s. 89.
([2]) Se skäl 64 i direktiv (EU) 2016/680.
([3]) Se det senaste målet Maximilian Schrems/Data Protection Commissioner (Schrems II), C-311/18, ECLI:EU:C:2020:559.
([4]) Se rekommendationer 01/2021 om referensramen för adekvat skyddsnivå enligt direktivet om uppgiftsskydd vid brottsbekämpning, som antogs i februari 2021 och finns på följande länk: https://edpb.europa.eu/our-work-tools/general-guidance/police-justice-guidelines-recommendations-best-practices_sv.
([5]) Mål C-362/14, Maximilian Schrems/Data Protection Commissioner (Schrems), ECLI:EU:C:2015:650, punkt 73.
([6]) *Schrems*-målet, punkt 74.
([7]) Meddelande från kommissionen till Europaparlamentet och rådet, Utbyte och skydd av personuppgifter i en globaliserad värld, COM(2017) 7 final, 10.1.2017, avsnitt 3.1, s. 6–7 som finns på följande länk: https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:52017DC0007&from=EN.

(5) Kommissionen har noggrant analyserat relevant lagstiftning och praxis i Förenade kungariket. På grundval av sina slutsatser nedan kommer kommissionen fram till att Förenade kungariket säkerställer en adekvat skyddsnivå för personuppgifter som överförs från behöriga myndigheter i unionen, som omfattas av tillämpningsområdet för direktiv (EU) 2016/680, till behöriga myndigheter i Förenade kungariket som omfattas av del 3 i *Data Protection Act 2018* (*dataskyddslagen från 2018*) ([8]).

(6) Detta beslut innebär att sådana överföringar får äga rum utan att det krävs ytterligare tillstånd för en period på fyra år, med förbehåll för en eventuell förlängning, och utan att det påverkar tillämpningen av de villkor som fastställs i artikel 35 i direktiv (EU) 2016/680.

2. REGLER FÖR BEHÖRIGA MYNDIGHETERS BEHANDLING AV PERSONUPPGIFTER I BROTTSBEKÄMPNINGSSYFTE

2.1 Den konstitutionella ramen

(7) Förenade kungariket är en parlamentarisk demokrati. Det har ett suveränt parlament som är högsta instans för alla andra statliga institutioner, en verkställande makt som är utvald av och ansvarig inför parlamentet och ett oberoende rättsväsende. Den verkställande makten bygger på dess förmåga att upprätthålla förtroendet i det valda underhuset och den är ansvarig inför båda kamrarna i parlamentet (underhuset och överhuset) som ansvarar för att granska regeringen samt debattera och stifta lagar. Förenade kungarikets parlament har delegerat ansvaret till det skotska parlamentet, det walesiska parlamentet (*Senedd Cymru*) och Nordirlands parlament för att lagstifta om vissa inhemska frågor i Skottland, Wales och Nordirland. Medan skydd av personuppgifter är en fråga som förbehålls Förenade kungarikets parlament, dvs. samma lagstiftning gäller i hela landet, har andra politikområden som är relevanta för detta beslut delegerats. Till exempel har Skottlands och Nordirlands straffrättsliga system, inklusive polisens verksamhet, delegerats till det skotska parlamentet respektive Nordirlands parlament ([9]).

(8) Även om Förenade kungariket inte har någon kodifierad konstitution i form av ett grundläggande konstituerande dokument har dess konstitutionella principer med tiden utvecklats, särskilt genom rättspraxis och konvention. Det konstitutionella värdet av vissa lagar, till exempel Magna Carta, 1689 års lag om rättigheter och lagen om mänskliga rättigheter från 1998 har erkänts. Enskilda personers grundläggande rättigheter har utvecklats, som en del av konstitutionen, genom gemensamma lagar, de skrivna lagarna och internationella fördrag, särskilt den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen), som Förenade kungariket ratificerade 1951. Förenade kungariket ratificerade även Europarådets konvention om skydd för enskilda personer vid automatisk databehandling av personuppgifter (konvention 108) 1987 ([10]).

(9) Genom *Human Rights Act 1998* införlivas de rättigheter som ingår i Europakonventionen i Förenade kungarikets lagstiftning. Lagen ger varje enskild person de grundläggande rättigheter och friheter som föreskrivs i artiklarna 2–12 och 14 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna och artiklarna 1–3 i dess första protokoll och artikel 1 i dess trettonde protokoll i jämförelse med artiklarna 16–18 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna. Detta inbegriper rätten till respekt för privatlivet och familjelivet som i sin tur omfattar rätten till skydd av personuppgifter och rätten till en rättvis rättegång ([11]). Enligt artikel 8 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna får en offentlig myndighet endast ingripa i rätten till privatliv enligt lagen om det är nödvändigt i ett demokratiskt samhälle för att skydda den nationella säkerheten, den allmänna säkerheten eller landets ekonomiska välstånd, för att förhindra oordning eller brott, för att skydda hälsa eller moral respektive för att skydda andras fri- och rättigheter.

([8]) Dataskyddslagen från 2018, finns på följande länk: https://www.legislation.gov.uk/ukpga/2018/12/contents.

([9]) *UK Explanatory Framework for Adequacy Discussion section F: Law enforcement*, finns på följande länk: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F_-_Law_Enforcement_.pdf.

([10]) Principerna i konvention 108 har ursprungligen införlivats i Förenade kungarikets lagstiftning genom dataskyddslagen från 1984 som har ersatts av dataskyddslagen från 1998 och därefter i sin tur av dataskyddslagen från 2018 (enligt den brittiska dataskyddsförordningen). Förenade kungariket har också undertecknat protokollet om ändring av konventionen om skydd för enskilda vid automatisk databehandling av personuppgifter (*konvention 108 +*) under 2018 och arbetar för närvarande med ratificeringen av konventionen.

([11]) Artiklarna 6 och 8 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (se även tillägg 1 till *Human Rights Act 1998*).

(10) I enlighet med *Human Rights Act 1998* måste alla åtgärder som vidtas av offentliga myndigheter vara förenliga med en rättighet som garanteras i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna ([12]). Dessutom måste primär- och sekundärrätten läsas och genomföras på ett sätt som är förenligt med dessa rättigheter ([13]). Om en enskild person anser att hans eller hennes rättigheter, inbegripet rätten till integritet och dataskydd, har kränkts av offentliga myndigheter, kan han eller hon få sin sak prövad av domstolar Förenade kungariket i enlighet med *Human Rights Act 1998* och slutligen, efter att ha uttömt nationella rättsmedel, få sin sak prövad av Europeiska domstolen för de mänskliga rättigheterna för kränkningar av de rättigheter som garanteras enligt Europakonventionen.

2.2 **Förenade kungarikets dataskyddsram**

(11) Den 31 januari 2020 utträdde Förenade kungariket ur unionen. På grundval av avtalet om Förenade konungariket Storbritannien och Nordirlands utträde ur Europeiska unionen och Europeiska atomenergigemenskapen ([14]) fortsatte unionsrätten att tillämpas i Förenade kungariket under övergångsperioden till och med den 31 december 2020. Före utträdet och under övergångsperioden bestod den rättsliga ramen för skydd av personuppgifter i Förenade kungariket för behöriga myndigheters behandling av personuppgifter för att förebygga, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inbegripet skydd mot och förebyggande av hot mot den allmänna säkerheten, av relevanta delar av 2018 års dataskyddslag genom vilken direktiv (EU) 2016/680 införlivades.

(12) Som en förberedelse inför utträdet ur EU antog Förenade kungarikets regering *European Union (Withdrawal) Act 2018* (EUWA) ([15]) som införlivade direkt tillämplig unionslagstiftning i Förenade kungarikets lagstiftning och föreskrev att så kallad EU-härledd inhemsk lagstiftning fortsätter att gälla efter övergångsperiodens slut. Del 3 i dataskyddslagen från 2018 ([16]) som införlivar direktiv (EU) 2016/680 utgör ”EU-härledd inhemsk lagstiftning” enligt EUWA. Enligt EUWA måste den oförändrade ”EU-härledda nationella lagstiftningen” tolkas av domstolarna i Förenade kungariket i enlighet med relevant rättspraxis från Europeiska unionens domstol och allmänna principer i unionsrätten eftersom de hade verkan omedelbart före övergångsperiodens utgång (*bibehållen EU-rättspraxis* respektive *bibehållen allmän EU-rättspraxis*) ([17]).

(13) Enligt EUWA har Förenade kungarikets ministrar befogenhet att införa sekundärlagstiftning via rättsliga instrument för att införa nödvändiga ändringar av bibehållen EU-lagstiftning till följd av Förenade kungarikets utträde ur unionen. Denna befogenhet utövades genom 2019 års förordningar om dataskydd, integritet och elektronisk kommunikation (ändringar etc.) (EU Exit) (DPPEC Regulations) ([18]). De ändrar Förenade kungarikets dataskyddslagstiftning, inklusive dataskyddslagen från 2018, så att den passar i den inhemska kontexten ([19]).

([12]) Avsnitt 6 i *Human Rights Act 1998*.

([13]) Avsnitt 3 i *Human Rights Act 1998*.

([14]) Avtalet om Förenade konungariket Storbritannien och Nordirlands utträde ur Europeiska unionen och Europeiska atomenergigemenskapen 2019/C 384 I/01, XT/21054/2019/INIT, EUT C 384I, 12.11.2019, s. 1 (*utträdesavtalet*) finns på följande länk: https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:12019W/TXT(02)&from=EN.

([15]) *European Union Withdrawal Act 2018* finns på följande länk: https://www.legislation.gov.uk/ukpga/2018/16/contents.

([16]) Dataskyddslagen från 2018, finns på följande länk: https://www.legislation.gov.uk/ukpga/2018/12/contents.

([17]) Avsnitt 6 i EUWA 2018.

([18]) 2019 års förordningar om dataskydd, integritet och elektronisk kommunikation (ändringar etc.) (EU Exit), finns på följande länk: https://www.legislation.gov.uk/uksi/2019/419/contents/made, ändrad av DPPEC 2020 som finns på följande länk: https://www.legislation.gov.uk/ukdsi/2020/9780348213522.

([19]) I *Exit Regulations* görs ett antal ändringar av del 3 i 2018 års dataskyddslag. Många av dessa är tekniska ändringar, t.ex. strykning av hänvisningar till ”medlemsstat” eller ”brottsbekämpningsdirektivet” (se t.ex. avsnitt 48.8 eller avsnitt 73.5 a i dataskyddslagen från 2018 med ”nationell lagstiftning”) så att del 3 fungerar effektivt som inhemsk lagstiftning efter övergångsperiodens slut. På vissa ställen krävdes andra typer av ändringar, till exempel när det gäller ”vem” antar ”beslut om adekvat skyddsnivå” i enlighet med Förenade kungarikets lagstiftning om skydd av personuppgifter (se avsnitt 74A i dataskyddslagen från 2018), dvs. den ansvariga ministern (Secretary of State) i stället för Europeiska kommissionen.

(14) Följaktligen kommer de rättsliga standarderna för behöriga myndigheters behandling av personuppgifter i syfte att förebygga, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inbegripet skydd mot och förebyggande av hot mot den allmänna säkerheten i Förenade kungariket efter övergångsperioden enligt utträdesavtalet att fortsätta att fastställas i relevanta delar av dataskyddslagen från 2018 men i dess ändrade lydelse enligt DPPEC-förordningarna, särskilt del 3 i den lagen. Den brittiska dataskyddsförordningen (UK GDPR) är inte tillämplig på denna typ av behandling.

(15) Del 3 i dataskyddslagen från 2018 innehåller regler för behandling av personuppgifter i brottsbekämpningssyfte, inbegripet dataskyddsprinciper, rättsliga grunder för behandling (laglighet), de registrerades rättigheter, de behöriga myndigheternas skyldigheter i egenskap av personuppgiftsansvariga och begränsningar av vidare överföringar. Samtidigt finns tillämpliga bestämmelser om tillsyn, verkställighet och prövning som är tillämpliga på den brottsbekämpande sektorn i delarna 5 och 6 i dataskyddslagen från 2018.

(16) Med tanke på polisstyrkornas relevanta roll inom den brottsbekämpande sektorn bör man dessutom beakta de regler som styr polisarbetet. Eftersom polisen är en decentraliserad angelägenhet är olika rättsakter, som dock ofta är snarlika till innehållet, tillämpliga på polisverksamhet i a) England och Wales, b) Skottland och c) Nordirland ([20]). Dessutom innehåller olika typer av vägledningsdokument ytterligare klargöranden om hur polisens befogenheter bör användas. Följande tre huvudsakliga former av polisvägledning finns: 1) Lagstadgad vägledning som utfärdats enligt lagstiftning, t.ex. *Code of Ethics* ([21]) och *Code of Practice on the Management of Police Information* (MoPI Code of Practice) ([22]) som utfärdats enligt *Police Act 1996* (polislagen från 1996) ([23]) eller Pace-koder ([24]) som utfärdats enligt *Police and Criminal Evidence Act* ([25]), 2) auktoriserad yrkesmässig praxis för hantering av polisinformation (*APP Guidance on the Management of Police Information*) ([26]) utfärdad av polishögskolan och 3) operativ vägledning (offentliggjord av polisen själv). *National Police Chiefs Council* (ett samordningsorgan för alla polisstyrkor i Förenade kungariket) offentliggör operativ vägledning som alla polisstyrkor har godkänt och som därför tillämpas nationellt ([27]). Syftet med denna vägledning är att säkerställa konsekvens mellan olika polisstyrkor när det gäller hur informationen hanteras ([28]).

(17) *MoPI Code of Practice* utfärdades av ministern 2005 med stöd av de befogenheter som föreskrivs i avsnitt 39A i polislagen från 1996 ([29]). Alla riktlinjer som utfärdas enligt polislagen måste godkännas av ministern och ska vara föremål för samråd med *National Crime Agency* innan de läggs fram för parlamentet. Enligt avsnitt 39A 7 i polislagen

([20]) För en mer detaljerad förklaring av polisstyrkorna och deras befogenheter i Förenade kungariket hänvisas till *UK Explanatory Framework for Adequacy Discussion section F: Law Enforcement* (se fotnot 9).

([21]) *Code of Practice for the Principles and Standards of Professional Behaviour for the Policing Profession of England and Wales* finns på följande länk: https://www.college.police.uk/What-we-do/Ethics/Documents/Code_of_Ethics.pdf; *Police Service Northern Ireland Code of Ethic* finns på följande länk: https://www.nipolicingboard.org.uk/psni-code-ethics; *Code of Ethic for police in Scotland* finns på följande länk: https://www.scotland.police.uk/about-us/code-of-ethics-for-policing-in-scotland/.

([22]) *Code of Practice on the Management of Police Information* finns på följande länk: http://library.college.police.uk/docs/APPref/Management-of-Police-Information.pdf.

([23]) Polislagen från 1996 finns på följande länk: https://www.legislation.gov.uk/ukpga/1996/16/contents.

([24]) Uppförandekoder enligt *Police and Criminal Evidence Act 1984* (Pace) finns på följande länk: https://www.gov.uk/guidance/police-and-criminal-evidence-act-1984-pace-codes-of-practice.

([25]) *Police and Criminal Evidence Act 1984* finns på följande länk: https://www.legislation.gov.uk/ukpga/1984/60/contents.

([26]) *Authorised Professional Practice on the Management of Police Information* finns på följande länk: https://www.app.college.police.uk/app-content/information-management/management-of-police-information/.

([27]) *Data Protection Manual for Police Data Protection Professionals* finns på följande länk: https://www.npcc.police.uk/2019%20FOI/IMORCC/225%2019%20NPCC%20DP%20Manual%20Draft%200.11%20Mar%202019.pdf.

([28]) Till exempel är *MoPI Code of Practice* (se fotnot 22) tillämplig på lagring av operativ polisinformation (se skäl (47) i detta beslut).

([29]) Enligt de uppgifter som lämnats av Förenade kungarikets myndigheter höll polishögskolan under perioden för samtal om adekvat skyddsnivå på att utarbeta en *Information and Records Management Code of Practice* som skulle ersätta MoPI. Utkastet till uppförandekod offentliggjordes för offentligt samråd den 25 januari 2021 och finns på följande länk: https://www.college.police.uk/article/information-records-management-consultation

ska polisen ta vederbörlig hänsyn till de uppförandekoder som utfärdats enligt lagen och därför förväntas polisen följa den ([30]). Dessutom måste den lagstadgade vägledningen (till exempel *APP Guidance on the Management of Police Information*) alltid vara förenlig med *MoPI Code of Practice* som återfinns ovanför den ([31]). Även om det kan finnas vissa operativa situationer där poliser behöver avvika från denna vägledning är de ändå skyldiga att uppfylla kraven i del 3 i dataskyddslagen från 2018 ([32]).

(18) Ytterligare vägledning om Förenade kungarikets dataskyddslagstiftning för behandling inom brottsbekämpningsområdet ges av Information Commissioner (*Information Commissioner* eller *Information Commissioner's Office*) ([33]) (för närmare uppgifter om *Information Commissioner's Office*, se skälen (93)–(109)). Även om det inte är rättsligt bindande skulle domstolarna i ett domstolsförfarande vara skyldiga att beakta eventuella överträdelser av riktlinjerna eftersom de har tolkningsvikt och visar hur dataskyddslagstiftningen tolkas och verkställs av Commissioner i praktiken ([34]).

(19) Som anges i skälen 8)–10) måste de brottsbekämpande organen i Förenade kungariket slutligen se till att Europakonventionen och konvention nr 108 följs.

(20) I sin struktur och sina huvudkomponenter är den rättsliga ramen för de brottsbekämpande myndigheternas behandling av uppgifter i Förenade kungariket således mycket lik den som gäller i EU. Detta inbegriper det faktum att en sådan ram inte enbart bygger på skyldigheter som föreskrivs i nationell rätt, som har utformats genom unionsrätten, utan även på skyldigheter som följer av internationell rätt, särskilt genom Förenade kungarikets anslutning till Europakonventionen och konvention 108 samt dess överlämnande till Europeiska domstolen för de mänskliga rättigheternas jurisdiktion. Dessa skyldigheter som följer av rättsligt bindande internationella instrument, särskilt när det gäller skydd av personuppgifter, är därför en särskilt viktig del av den rättsliga ram som bedöms i detta beslut.

2.3 **Materiellt och territoriellt tillämpningsområde**

(21) Det materiella tillämpningsområdet för del 3 i dataskyddslagen från 2018 sammanfaller med tillämpningsområdet för direktiv 2016/680 enligt artikel 2.2 i samma direktiv. Del 3 ska tillämpas på en behörig myndighets behandling av personuppgifter helt eller delvis på automatisk väg och på en behörig myndighets behandling på annat sätt än automatiserad behandling av personuppgifter som ingår i eller är avsedda att ingå i ett register.

(22) För att omfattas av del 3 måste den personuppgiftsansvariga vara en ”behörig myndighet” och behandlingen måste utföras för ett ”brottsbekämpande ändamål”. Därför är det system för skydd av personuppgifter som bedöms i detta beslut tillämpligt på all brottsbekämpande verksamhet som bedrivs av dessa behöriga myndigheter.

(23) Begreppet ”behörig myndighet” definieras i avsnitt 30 i dataskyddslagen som en person som förtecknas i tillägg 7 till dataskyddslagen från 2018 samt varje annan person i den mån personen har lagstadgade uppgifter för något av de brottsbekämpande ändamålen. De behöriga myndigheter som förtecknas i tillägg 7 omfattar inte bara polisen utan även alla ministerier och andra myndigheter med utredningsfunktioner (t.ex. *Commissioner for Her Majesty's Revenue*

([30]) I målet R/Commission of Police of the Metropolis [2014] EWCA Civ 585 bekräftades den juridiska statusen för *MoPI Code of Practice* och *Lord Justice Laws* förklarade att Metropolitan Police Commissioner är skyldig att beakta *MoPI Code of Practice* och *APP Guidance on Management of Police Information* i enlighet med avsnitt 39A i polislagen från 1996.

([31]) Polisen inspekteras med avseende på efterlevnaden av *MoPI Code of Practice* av *Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services* (HMICFRS).

([32]) Se i detta avseende polisakademins (*College of Policing*) ståndpunkt om efterlevnaden av APP:s riktlinjer för alla delar av polisarbetet, där det förklaras att ”APP är auktoriserat av det professionella polisorganet (*College of Policing*) som den officiella källan till yrkesmässig praxis inom polisväsendet. Poliser och personal förväntas ta hänsyn till auktoriserad yrkesmässig praxis när de fullgör sina skyldigheter. Det kan dock finnas omständigheter där det finns legitima operativa skäl för att en styrka avviker från auktoriserad yrkesmässig praxis under förutsättning att det finns en tydlig motivering till detta. Styrkan skulle ha ansvaret för alla lokala och nationella risker som hänger samman med att verka utanför nationellt överenskomna riktlinjer och om en incident inträffar eller en utredning görs som en följd av detta (t.ex. genom Independent Office of Police Conduct) är styrkan ansvarig för alla risker”, information om detta finns på följande länk: https://www.app.college.police.uk/faq-page/.

([33]) *Guide to Law Enforcement Processing* finns på följande länk: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/.

([34]) Se domen i målet Bridges/Chief Constable of South Wales Police [2019] EWHC 2341 (Admin), där High Court, trots att den noterade att Commissioner's riktlinjer inte var lagenliga, angav att ”med tanke på om en registeransvarig har uppfyllt sin skyldighet enligt avsnitt 64 [att genomföra en konsekvensbedömning avseende dataskydd i samband med behandling med hög risk] kommer en domstol att ta hänsyn till den vägledning som har utfärdats av Information Commissioner i fråga om konsekvensbedömningar avseende dataskydd”.

and Customs, the Welsh Revenue Authority, the Competition and Markets Authority, Her Majesty's Land Register eller *the National Crime Agency*), åklagarmyndigheter, andra straffrättsliga myndigheter och andra innehavare eller organisationer som bedriver brottsbekämpande verksamhet i Förenade kungariket ([35]). Del 3 i dataskyddslagen från 2018 är också tillämplig på domstolar när de utövar sina rättsliga funktioner med undantag för den del som rör den registrerades rättigheter och tillsyn av ICO (kontoret för *Information Commissioner*) ([36]). Förteckningen över behöriga myndigheter i tillägg 7 är inte slutgiltig och kan uppdateras av ministern genom förordningar som tar hänsyn till förändringar i organisationen av offentliga ämbeten ([37]).

(24) Behandlingen i fråga måste också ha ett ”brottsbekämpningssyfte” som definieras som förebyggande, utredning, avslöjande eller lagföring av brott eller verkställighet av straffrättsliga påföljder, inbegripet skydd mot och förebyggande av hot mot den allmänna säkerheten ([38]). Behandling som utförs av en behörig myndighet regleras inte av del 3 i dataskyddslagen från 2018 om behandlingen inte sker i brottsbekämpande syfte. Detta kommer till exempel att vara fallet när konkurrens- och marknadsmyndigheten utreder ärenden som inte är kriminaliserade (t. ex. företagssammanslagningar). I så fall kommer den brittiska dataskyddsförordningen (UK GDPR), tillsammans med del 2 i dataskyddslagen från 2018, att gälla eftersom behöriga myndigheters behandling av personuppgifter sker för andra ändamål än brottsbekämpning. För att avgöra vilket system för skydd av personuppgifter som ska tillämpas (del 3 eller del 2 i dataskyddslagen från 2018) på behandlingen av personuppgifter i fråga måste den behöriga myndigheten, dvs. den personuppgiftsansvariga, överväga om det ”primära ändamålet” med sådan behandling är ett av de brottsbekämpande ändamålen enligt dataskyddslagen från 2018.

(25) När det gäller det territoriella tillämpningsområdet för del 3 i dataskyddslagen från 2018 föreskrivs i avsnitt 207.2 att dataskyddslagen är tillämplig på behandling av personuppgifter i samband med verksamhet som bedrivs av en person som har en etablering inom hela Förenade kungarikets territorium. Detta inbegriper offentliga myndigheter i territorierna England, Wales, Skottland och Nordirland som omfattas av det materiella tillämpningsområdet av del 3 i dataskyddslagen från 2018 ([39]).

2.3.1 *Definition av personuppgifter och behandling*

(26) De viktigaste begreppen personuppgifter och behandling definieras i avsnitt 3 i dataskyddslagen från 2018 och gäller i hela dataskyddslagen. Definitionerna följer nära motsvarande definitioner i artikel 3 i direktiv 2016/680. Enligt dataskyddslagen från 2018 avses med personuppgifter all information som avser en identifierad eller identifierbar fysisk person ([40]). Enligt avsnitt 3.3 i dataskyddslagen från 2018 är en individ identifierbar om han eller hon direkt eller indirekt kan identifieras utifrån informationen, inbegripet genom hänvisning till ett namn eller en identifierare eller genom hänvisning till en eller flera faktorer som är specifika för personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet. Begreppet ”behandling” definieras som en åtgärd eller serie av åtgärder som utförs på information eller på en uppsättning uppgifter, till exempel a) insamling, registrering, organisering, strukturering eller lagring, b) anpassning eller ändring, c) hämtning, läsning eller användning, d) utlämnandet genom överföring, spridning eller på annat sätt tillgängliggörande, e) inställning eller kombination eller f) begränsning, radering eller förstöring. I lagen definieras dessutom ”känslig behandling” som ”a) behandling av personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening, b) behandling av genetiska uppgifter eller biometriska uppgifter i syfte att unikt identifiera en individ, c) behandling av hälsouppgifter, d) behandling av uppgifter om en persons sexualliv eller sexuella läggning” ([41]). I detta avseende innehåller avsnitt 205 i dataskyddslagen från 2018 en definition av ”biometriska uppgifter” ([42]), ”uppgifter om hälsa” ([43]) och ”genetiska uppgifter” ([44]).

([35]) Bland dessa förtecknas Directors of Public Prosecutors, Director of Public Prosecutors for Northern Ireland eller Information Commission i tillägg 7 till dataskyddslagen från 2018.

([36]) Avsnitt 43.3 i dataskyddslagen från 2018.

([37]) Avsnitt 30.3 i dataskyddslagen från 2018. Underrättelsetjänsterna (*Secret Intelligence Service*, *Security Service* och *Government Communications Headquarters*) är inte behöriga myndigheter (se avsnitt 30.2 i dataskyddslagen från 2018) och del 3 i dataskyddslagen från 2018 är inte tillämplig på någon av deras verksamheter. Deras verksamhet omfattas av del 4 i dataskyddslagen från 2018.

([38]) Avsnitt 31 i dataskyddslagen från 2018.

([39]) Detta innebär att dataskyddslagen från 2018 och därmed detta beslut inte är tillämpliga på Förenade kungarikets kronbesittningar och Förenade kungarikets övriga utomeuropeiska territorier, exempelvis Falklandsöarna och territoriet Gibraltar.

([40]) Personuppgifter som rör avlidna personer omfattas inte av dataskyddslagen från 2018.

([41]) Avsnitt 35.8 i dataskyddslagen från 2018.

([42]) Biometriska uppgifter innebär personuppgifter som härrör från en specifik teknisk behandling som rör en persons fysiska, fysiologiska eller beteendemässiga egenskaper och som möjliggör eller bekräftar en unik identifiering av den personen, till exempel ansiktsbilder eller fingeravtrycksuppgifter.

([43]) Uppgifter om hälsa innebär personuppgifter om en persons fysiska eller psykiska hälsa, inbegripet hälso- och sjukvårdstjänster, som avslöjar information om personens hälsotillstånd.

([44]) Genetiska uppgifter innebär personuppgifter som rör en individs ärvda eller förvärvade genetiska egenskaper och som ger unik information om den personens fysiologi eller hälsa och som i synnerhet är resultatet av en analys av ett biologiskt prov från den berörda personen.

(27) I avsnitt 32 i dataskyddslagen från 2018 förtydligas definitionerna av registeransvarig och personuppgiftsbiträde i samband med behandling av personuppgifter för brottsbekämpande ändamål i enlighet med motsvarande definitioner i direktiv 2016/680. Den personuppgiftsansvariga innebär den behöriga myndighet som fastställer ändamålen och medlen för behandlingen av personuppgifter. Om behandlingen krävs enligt lag är den personuppgiftsansvariga den behöriga myndighet för vilken en sådan skyldighet föreskrivs i den aktuella lagen. Ett personuppgiftsbiträde definieras som varje person som behandlar personuppgifter för den personuppgiftsansvarigas räkning (utom en person som är anställd hos den personuppgiftsansvariga).

2.4 **Skyddsåtgärder, rättigheter och skyldigheter**

2.4.1 *Laglig och korrekt behandling*

(28) Enligt avsnitt 35 i dataskyddslagen från 2018 ska behandlingen av personuppgifter vara laglig och rättvis på ett liknande sätt som i artikel 4.1 a i direktiv (EU) 2016/680. I enlighet med avsnitt 35.2 i dataskyddslagen från 2018 är behandling av personuppgifter för något av de brottsbekämpande ändamålen laglig endast om den grundas på lag och den registrerade har gett sitt samtycke till behandlingen för detta ändamål eller om behandlingen är nödvändig för att utföra en arbetsuppgift som utförs för detta ändamål av en behörig myndighet.

2.4.1.1 Behandling på grundval av lag

(29) I likhet med artikel 8 i direktiv (EU) 2016/680 måste sådan behandling grundas på lag för att säkerställa att en behandling som omfattas av del 3 i dataskyddslagen från 2018 är laglig. Laglig behandling innebär tillåten enligt antingen lag, gemensam lag eller kungliga befogenheter ([45]).

(30) De behöriga myndigheternas befogenheter regleras i allmänhet av stadgar vilket innebär att deras uppgifter och befogenheter tydligt anges i lagstiftning som antas av parlamentet ([46]). I vissa fall kan polisen och andra behöriga myndigheter som förtecknas i tillägg 7 i dataskyddslagen från 2018 förlita sig på common law för att behandla uppgifter ([47]). Common law har byggts upp genom prejudikat i domstolsbeslut. Common law är relevant inom ramen för polisens befogenheter som härrör från denna rättskälla och dess grundläggande skyldighet att skydda allmänheten genom att upptäcka och förebygga brott ([48]). Polisen har dock befogenheter både när det gäller common law och

([45]) Förklarande anmärkningar till dataskyddslagen från 2018, punkt 181, finns på följande länk: https://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpgaen_20180012_en.pdf.

([46]) National Crime Agency härleder till exempel sina befogenheter från *Crime and Courts Act 2013* som finns på följande länk: https://www.legislation.gov.uk/ukpga/2013/22/contents. Food Standards Agency's befogenheter regleras också i *Food Standards Act 1999* som finns på följande länk: https://www.legislation.gov.uk/ukpga/1999/28/contents. Andra exempel är lagen *Prosecution of Offenders Act 1985* genom vilken Crown Prosecution Service inrättades (se https://www.legislation.gov.uk/ukpga/1985/23/contents)), *Commissioners for Revenue and Customs Act* 2005 genom vilken skatte- och tullmyndigheten(*Her Majesty's Revenue and Customs*) inrättades (se https://www.legislation.gov.uk/ukpga/2005/11/contents), *Criminal Procedure (Scotland) Act 1995* genom vilken Scottish Criminal Cases Review Commission inrättades (se https://www.legislation.gov.uk/ukpga/1995/46/contents)), *Justice (Northern Ireland) Act 2002* genom vilken Public Prosecution Service in Northern Ireland inrättades (se https://www.legislation.gov.uk/ukpga/2002/26/contents) och Serious Fraud Office skapades och fick sina befogenheter enligt strafflagen från 1987 (*Criminal Justice Act 1987*) (se https://www.legislation.gov.uk/ukpga/1987/38/contents).

([47]) Enligt de uppgifter som lämnats av Förenade kungarikets myndigheter får exempelvis Lord Advocate, som är chef för åklagarsystemet i Skottland, inom Crown Office and Procurator Fiscal Service, som ansvarar för lagföring av mål i Skottland, sina befogenheter att utreda dödsfall och lagföra brott från common law medan en del av hans eller hennes funktion är fastställd i lag. Dessutom härleder kronan och i förlängningen olika ministerier, departement och ministrar också sina befogenheter från en kombination av lagstiftning, common law och kungligt prerogativ (detta innebär gemensamma rättsliga befogenheter som tillhör kronan men utövas av ministrar).

([48]) *UK Explanatory Framework for adequacy Discussion section F: Law Enforcement*, s. 8 (se fotnot 9).

lagstiftning ([49]) för att fullgöra en sådan skyldighet. Om polisen har en lagstadgad befogenhet ersätter detta alla befogenheter enligt common law ([50]).

(31) Omfattningen av polistjänstemannens befogenheter och skyldigheter enligt common law har av domstolarna erkänts omfatta ”alla åtgärder som han eller hon anser nödvändiga för att upprätthålla den allmänna ordningen, förhindra brott eller skydda egendom mot kriminella handlingar” ([51]). Befogenheter enligt common law är inte oreserverade befogenheter. De omfattas av en rad begränsningar, däribland gränser som fastställts av domstolarna ([52]) och genom lagstiftning, särskilt *Human Rights Act 1998* och 2010 års lag om jämställdhet (*Equality Act 2010*) ([53]). För behöriga myndigheter som behandlar uppgifter enligt del 3 i dataskyddslagen från 2018 innebär detta dessutom att de utövar befogenheter enligt common law i enlighet med kraven i dataskyddslagen från 2018 ([54]). Dessutom måste ett beslut om att utföra någon form av databehandling beakta kraven i tillämplig vägledning, till exempel *MoPI Code of Practice* och vägledning som är specifik för ett av Förenade kungarikets länder ([55]). Regeringen och det operativa polisväsendet utfärdar ett antal vägledningsdokument för att se till att poliser utövar sina befogenheter inom de gränser som fastställs i common law eller annan relevant lagstiftning ([56]).

(32) Kungliga befogenheter utgör en annan del av ”lagen” och hänvisar till vissa befogenheter som kronan har som kan utövas av den verkställande makten som inte grundar sig på lag utan härrör från monarkens suveränitet ([57]). Det finns mycket få exempel på särskilda befogenheter som är relevanta i brottsbekämpningssammanhang. De omfattar till exempel en ram för ömsesidig rättslig hjälp som gör det möjligt för en minister att utbyta uppgifter med tredjeländer för brottsbekämpande ändamål och befogenheten att dela uppgifter på detta sätt fastställs inte alltid i

([49]) De viktigaste rättsakterna om de viktigaste polisiära befogenheterna (gripande, husrannsakan, tillstånd till fortsatt frihetsberövande, fingeravtryck, tagande av intima prover, beslut om avlyssning, tillgång till kommunikationsuppgifter) är följande: i) För England och Wales, Police and *Criminal Evidence Act 1984* (Pace) som finns på följande länk https://www.legislation.gov.uk/ukpga/1984/60/contents (ändrad genom *Protection of Freedoms Act 2012* (PoFA) som finns på följande länk: https://www.legislation.gov.uk/ukpga/2012/9/contents) och 2016 års lag om utredningsbefogenheter (IPA) som finns på följande länk: https://www.legislation.gov.uk/ukpga/2016/25/contents), ii) för *Skottland, Criminal Justice (Scotland) Act 2016* som finns på följande länk: https://www.legislation.gov.uk/asp/2016/1/contents och *Criminal Procedure (Scotland) Act 1995* som finns på följande länk: https://www.legislation.gov.uk/ukpga/1995/46/contents) iii) för *Northern Ireland, Police and Criminal Evidence (Northern Ireland) Order 1989* som finns på följande länk: https://www.legislation.gov.uk/nisi/1989/1341/contents.

([50]) Förenade kungarikets myndigheter har förklarat att författningsrättens företräde sedan länge är etablerat i Förenade kungariket, ända sedan domen i målet Entick/Carrington [1765] EWHC KB J98 bekräftade att det finns begränsningar för den verkställande maktens utövande av befogenheter och fastställde principen att monarkens och regeringens särskilda befogenheter och befogenheter enligt common law är underordnade landets lagstiftning.

([51]) Se målet Rice/Connolly [1966] 2 QB 414.

([52]) Se målet R (Catt)/Association of Chief Police Officers [2015] AC 1065, där Lord Sumption, när det gäller polisens befogenhet att inhämta och lagra information om en person (som hade begått ett brott), ansåg att polisen enligt common law har befogenhet att inhämta och lagra information för polisändamål, dvs. generellt sett för att upprätthålla allmän ordning samt förebygga och upptäcka brott. Dessa befogenheter tillåter inte inkräktande metoder för inhämtande av information, till exempel intrång på privat egendom eller handlingar (andra än gripanden enligt common law-befogenheter) som skulle utgöra ett angrepp. Domaren ansåg att det i detta fall räckte med befogenheter enligt common law för att tillåta inhämtande och lagring av den typ av offentlig information som kommer i fråga för dessa överklaganden.

([53]) 2010 års lag om jämställdhet finns på följande länk: https://www.legislation.gov.uk/ukpga/2010/15/contents.

([54]) För ett exempel på ett fall där polisens gemensamma befogenheter bedöms inom ramen för dataskyddslagen från 1998, se High Courts beslut i Bridges/Chief Constable of South Wales Police (se fotnot 33). Se även målen Vidal-Hall/Google Inc [2015] EWCA Civ 311 och Richard/BBC [2018] EWHC 1837 (Ch).

([55]) Se till exempel vägledning från Police Service of Northern Ireland om instruktioner för dokumenthantering som finns på följande länk: https://www.psni.police.uk/globalassets/advice–information/our-publications/policies-and-service-procedures/records-management-080819.pdf.

([56]) Underhuset har publicerat ett informationsdokument som beskriver polisens viktigaste befogenheter enligt common law och lagstadgade befogenheter i England och Wales (se https://researchbriefings.files.uk/documents/CBP-8637/CBP-8637.pdf). Enligt detta dokument är exempelvis befogenheterna att upprätthålla ”kronans fred” och ”användning av våld” härleds från common law men ”stopp- och sökbefogenheterna” härleds alltid från lagstiftningen. Dessutom tillhandahåller den skotska regeringen information på sin webbplats om polisens befogenheter att gripa och stoppa (se https://www.gov.scot/policies/police/police-powers/).

([57]) Enligt den information som lämnats av Förenade kungarikets myndigheter omfattar de särskilda befogenheter som regeringen utövar till exempel att ingå och ratificera fördrag, genomföra diplomati och använda de väpnade styrkorna i Förenade kungariket för att upprätthålla freden till stöd för polisen.

lag ([58]). Kungliga befogenheter är bundna av common law-principerna ([59]), är underordnade lagen och omfattas därför av de begränsningar som anges i *Human Rights Act 1998* och dataskyddslagen från 2018 ([60]).

(33) I likhet med artikel 8 i direktiv (EU) 2016/680 kräver systemet i Förenade kungariket att de behöriga myndigheterna för att följa principen om laglighet ser till att behandlingen, när den grundar sig på lagen, också måste vara ”nödvändig” för att fullgöra den uppgift som utförs i brottsbekämpningssyfte. ICO ger vägledning i detta avseende och klargör att ”det måste vara ett riktat och proportionerligt sätt att uppnå syftet. Den rättsliga grunden gäller inte om du rimligtvis kan uppnå syftet med något annat mindre inkräktande medel. Det räcker inte att hävda att behandlingen är nödvändig eftersom du har valt att driva din verksamhet på ett visst sätt. Frågan är om behandlingen är nödvändig för det angivna ändamålet ([61])”.

2.4.1.2. Behandling på grundval av den registrerades ”samtycke”

(34) Enligt skäl (28) ger avsnitt 35.2 i dataskyddslagen från 2018 möjlighet att behandla personuppgifter på grundval av den enskildas ”samtycke”.

(35) Samtycke förefaller dock inte vara en rättslig grund som är relevant för den behandling som omfattas av detta beslut. Den behandling som omfattas av detta beslut kommer i själva verket alltid att gälla uppgifter som har överförts av en behörig myndighet i en medlemsstat till en behörig myndighet i Förenade kungariket enligt direktiv (EU) 2016/680. Därför omfattar de vanligtvis inte den typ av direkt interaktion (insamling) mellan en offentlig myndighet och registrerade personer som kan baseras på samtycke enligt avsnitt 35.2 a i dataskyddslagen från 2018.

(36) Även om åberopande av samtycke därför inte anses relevant för den bedömning som görs enligt detta beslut bör det för fullständighetens skull noteras att behandling i brottsbekämpningssammanhang aldrig grundar sig enbart på samtycke eftersom en behörig myndighet alltid måste ha en underliggande befogenhet som gör det möjligt för den att behandla uppgifterna ([62]). Mer specifikt, och i likhet med vad som är tillåtet enligt direktiv (EU) 2016/680 ([63]), innebär detta att samtycke fungerar som ett ytterligare villkor för att möjliggöra vissa begränsade och specifika behandlingar som annars inte skulle kunna utföras, till exempel insamling och behandling av ett DNA-prov från en individ som inte är misstänkt. I detta fall skulle behandlingen inte utföras om medgivandet inte ges eller återkallas ([64]).

([58]) Se i detta avseende bedömningen av Förenade kungarikets system för vidare överföring i skälen (74)-(87).

([59]) Se målet Bancoult/Secretary of State for Foreign and Commonwealth Affairs [2008] UKHL 61, där domstolarna ansåg att befogenheten enligt prerogativ att utfärda förvaltningsföreskrifter också omfattades av de vanliga rättsliga grunderna.

([60]) Se målet Attorney-General/De Keyser's Royal Hotel Ltd [1920] [1920] AC 508 där domstolen slog fast att särskilda befogenheter inte kan utnyttjas när lagstadgade befogenheter ersätter dem. Målet Laker Airways Ltd/Department of Trade 1977] QB 643,] där domstolen fann att särskilda befogenheter inte kan användas för att motverka lagbestämmelser. Målet R/Secretary of State for the Home Department, ex p. Fire Brigades Union [1995] UKHL 3 där domstolen slog fast att särskilda befogenheter inte kan utnyttjas när de strider mot antagen lagstiftning, även om den antagna lagstiftningen ännu inte har trätt i kraft. Målet R (Miller)/Secretary of State for Exiting the European Union [2017] UKSC 5 där domstolen bekräftade att den skrivna lagen kan ändra och avskaffa särskilda befogenheter. För en allmän översikt över förhållandet mellan de kungliga befogenheterna och stadgeenliga befogenheter eller befogenheter enligt common law, se underhusets briefingdokument som finns på följande länk: https://researchbriefings.files.parliament.uk/documents/SN03861/SN03861.pdf.

([61]) *Guide to Law Enforcement Processing, "What is the first principle about?"* finns på följande länk: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/principles/#ib2.

([62]) Detta följer av lydelsen i den relevanta bestämmelsen i dataskyddslagen från 2018, enligt vilken behandling av personuppgifter för något av de brottsbekämpande ändamålen är laglig endast om och i den mån som ”den grundas på lag” och att a) den registrerade personen har gett sitt samtycke till behandlingen för detta ändamål eller b) behandlingen är nödvändig för att utföra en arbetsuppgift som fullgörs av en behörig myndighet för detta ändamål.

([63]) Se skälen 35 och 37 i direktiv (EU) 2016/680.

([64]) Förenade kungarikets myndigheter har förklarat att ett exempel på när samtycke kan vara en lämplig grund för behandling skulle vara om polisen erhåller ett DNA-prov i samband med en försvunnen person för att matcha mot en kropp om en sådan påträffas. Under sådana omständigheter skulle det vara olämpligt för polisen att tvinga den registrerade att lämna ett prov. I stället skulle polisen begära den enskildas samtycke, som ges frivilligt och när som helst kan återkallas. Om samtycke återkallas kan uppgifterna inte längre behandlas såvida inte en ny rättslig grund har fastställts för att fortsätta att behandla provet (t.ex. att den registrerade blev en misstänkt person). Ett annat exempel kan vara när en polisstyrka utreder ett brott där ett brottsoffer (det kan vara ett offer för ett rån, sexualbrott, våld i hemmet, släktingar till ett mordoffer eller annat brottsoffer) skulle kunna dra nytta av en hänvisning till *Victim Support* (en oberoende välgörenhetsorganisation som ger stöd till människor som drabbats av brott och traumatiska händelser). Under sådana omständigheter kommer polisen endast att dela personlig information med *Victim Support*, t.ex. namn och kontaktuppgifter, om brottsoffret ger sitt samtycke.

(37) I fall där det krävs samtycke från den enskilda måste samtycket vara otvetydigt och innebära en entydig bekräftande handling ([65]). Polisen måste ha ett meddelande om skydd av personuppgifter som bland annat innehåller nödvändig information om giltig användning av samtycke. Dessutom offentliggör vissa av dem ytterligare material om hur de följer dataskyddslagstiftningen, inklusive hur och när de skulle använda samtycke som rättslig grund ([66]).

2.4.1.3. Känslig behandling

(38) Specifika skyddsåtgärder bör vidtas när ”särskilda kategorier av uppgifter” behandlas. I detta avseende innehåller del 3 i dataskyddslagen från 2018 starkare skyddsåtgärder för så kallad känslig behandling i likhet med vad som föreskrivs i artikel 10 i direktiv (EU) 2016/680 ([67]).

(39) Enligt avsnitt 35.3 i dataskyddslagen från 1998 får känsliga uppgifter behandlas av behöriga myndigheter för brottsbekämpande ändamål endast i följande två fall: 1) Den registrerade har gett sitt samtycke till behandlingen för brottsbekämpande ändamål och vid den tidpunkt då behandlingen utförs har den personuppgiftsansvariga infört ett välvalt policydokument ([68]). 2) Behandlingen är absolut nödvändig för det brottsbekämpande ändamålet, behandlingen uppfyller minst ett av villkoren i tillägg 8 till dataskyddslagen från 2018 och vid den tidpunkt då behandlingen utförs har den personuppgiftsansvariga ett välvalt policydokument på plats ([69]).

(40) När det gäller det första fallet och enligt förklaringen i skäl 38 anses åberopande av samtycke inte vara relevant för den typ av överföringssituation som omfattas av detta beslut ([70]).

(41) Om behandlingen av känsliga uppgifter inte bygger på samtycke kan den utföras enligt något av de villkor som anges i tillägg 8 till dataskyddslagen från 2018. Dessa villkor avser behandling som är nödvändig för lagstadgade ändamål som rättskipning, skyddet av intressen som är av grundläggande betydelse för den registrerade personen eller för en annan enskild, skydd av barn och riskutsatta personer, rättsliga anspråk, rättshandlingar, förebyggande av bedrägerier och arkivering om personuppgifterna på ett uppenbart sätt offentliggörs av den registrerade personen. Bortsett från det fall då uppgifterna på ett uppenbart sätt offentliggörs är alla villkor i tillägg 8 föremål för ett ”strikt

([65]) Det finns ingen separat definition av ”samtycke” för behandling av personuppgifter enligt del 3 i dataskyddslagen från 2018. ICO gav vägledning om begreppet ”samtycke” i del 3 i dataskyddslagen från 2018 och klargjorde att det har samma innebörd och bör anpassas till den definition som ges i dataskyddsförordningen, särskilt att ”samtycket måste vara frivilligt, specifikt och informerat och att det måste finnas ett genuint val att samtycka till de uppgifter som behandlas” (*Guide to Law Enforcement Processing, ”What is the first principle about?”* (se fotnot 64) och *Guide to Data Protection on consent* som finns på följande länk: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/).

([66]) Se till exempel informationen på Lincolnshire police webbplats (se https://www.lincs.police.uk/resource-library/data-protection/law-enforcement-processing/) eller på West Yorkshire Police webbplats (se https://www.westyorkshire.police.uk/sites/default/files/2018-06/data_protection.pdf).

([67]) Avsnitt 35.8 i dataskyddslagen från 2018.

([68]) Avsnitt 35.4 i dataskyddslagen från 2018.

([69]) Avsnitt 35.5 i dataskyddslagen från 2018.

([70]) För fullständighetens skull är det värt att notera att när behandling grundar sig på samtycke måste den ges frivilligt, vara specifik och informerad och det måste finnas ett specifikt val att samtycka till de uppgifter som behandlas. Dessutom måste den personuppgiftsansvariga ha ett ”välvalt policydokument” när behandling sker på grundval av den registrerades samtycke. I avsnitt 42 i dataskyddslagen från 2018 beskrivs de krav som det välvalda policydokumentet måste uppfylla. Det klargörs att dokumentet åtminstone måste förklara den personuppgiftsansvarigas förfaranden för att säkerställa överensstämmelse med dataskyddsprinciperna och förklara den personuppgiftsansvarigas policy när det gäller lagring och radering av personuppgifter. Enligt avsnitt 42 i dataskyddslagen från 2018 innebär detta att den personuppgiftsansvariga måste lägga fram en handling som a) förklarar den personuppgiftsansvarigas förfaranden för att säkerställa överensstämmelse med dataskyddsprinciperna och b) förklarar den personuppgiftsansvarigas policy för lagring och radering av personuppgifter som behandlas i enlighet med den registrerades samtycke eller anger hur länge sådana personuppgifter sannolikt kommer att lagras. I policydokumentet krävs särskilt att den personuppgiftsansvariga alltid ska inkludera de delar som nämns i leden a) och b) när han eller hon fullgör sin skyldighet att registrera behandlingen. ICO har publicerat ett malldokument (*Guide to Law Enforcement Processing*. *”Conditions for sensitive processing”* som finns på följande länk: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/conditions-for-sensitive-processing) och kan vidta verkställande åtgärder om de personuppgiftsansvariga inte uppfyller dessa krav. Det välvalda policydokumentet ska prövas i domstolar när man beaktar potentiella överträdelser av dataskyddslagen från 2018. I målet R (Bridges)/Chief Constable of South Wales Police nyligen granskade domstolarna till exempel den personuppgiftsansvarigas välvalda policydokument och fann att det var tillräckligt men skulle ha dragit nytta av ytterligare detaljer. Till följd av detta såg polisen i South Wales över det välvalda policydokumentet och uppdaterade det i enlighet med ICO:s nya vägledning (se fotnot 33). I enlighet med avsnitt 42.3 i dataskyddslagen från 2018 bör dessutom det välvalda policydokumentet regelbundet ses över av den personuppgiftsansvariga. Slutligen är den personuppgiftsansvariga, som ytterligare en skyddsåtgärd, enligt avsnitt 42.4 i dataskyddslagen från 2018 skyldig att föra ett utökat register över behandlingen, inklusive ytterligare element jämfört med den allmänna skyldighet som åligger den personuppgiftsansvariga att föra register över den behandling som anges i avsnitt 61 dataskyddslagen från 2018.

nödvändighetstest". ICO har klargjort att "det är absolut nödvändigt i detta sammanhang att behandlingen måste avse ett trängande socialt behov och att du inte rimligen kan uppnå det med mindre inkräktande medel" ([71]). Vissa villkor är dessutom föremål för ytterligare begränsningar. För att exempelvis åberopa villkoret om "lagstadgade ändamål" och "skyddsvillkoret" (tillägg 8, punkt 1 och punkt 4) finns det ytterligare ett kriterium av allmänt intresse som måste uppfyllas. När det gäller villkoren för skydd av barnet (tillägg 8, punkt 4) måste den registrerade dessutom vara av en viss ålder och anses vara utsatt för risk. Dessutom kan den personuppgiftsansvariga endast tillämpa villkoret i punkt 4 i tillägg 8 under särskilda omständigheter ([72]). På samma sätt finns det begränsningar för villkoren för "rättsliga handlingar" och "förebyggande av bedrägeri" (tillägg 8, punkt 7 respektive 8). Båda är endast tillämpliga på specifika personuppgiftsansvariga. När det gäller rättsliga handlingar får endast en domstol eller annan rättslig myndighet använda ett sådant villkor och, när det gäller bedrägeribekämpning, kan endast personuppgiftsansvariga som är bedrägeribekämpningsorganisationer förlita sig på detta villkor.

(42) När behandlingen bygger på något av de villkor som anges i tillägg 8 respektive avsnitt 42 i dataskyddslagen från 2018 måste det finnas ett "välvalt policydokument" som förklarar den personuppgiftsansvarigas förfaranden för att säkerställa efterlevnad av dataskyddsprinciperna och den personuppgiftsansvarigas policy för lagring och radering av personuppgifter samt att utökade registerskyldigheter gäller.

2.4.2 *Ändamålsbegränsning*

(43) Personuppgifter ska behandlas för ett specifikt ändamål och därefter användas endast i den utsträckning som detta är förenligt med behandlingens ändamål. Denna princip om skydd av personuppgifter garanteras genom avsnitt 36 i dataskyddslagen från 2018. Denna bestämmelse kräver, i likhet med artikel 4.1 b i direktiv (EU) 2016/680, att a) det brottsbekämpande ändamål för vilket personuppgifter samlas in vid varje tillfälle ska specificeras, vara uttryckligt och legitimt och b) att personuppgifter som samlas in på detta sätt inte får behandlas på ett sätt som är oförenligt med det syfte för vilket de samlades in.

(44) När behöriga myndigheter behandlar uppgifter för brottsbekämpande ändamål kan detta inbegripa arkivering, vetenskaplig eller historisk forskning och statistiska ändamål ([73]). I dessa fall klargör dataskyddslagen från 2018 också att arkivering (eller behandling för vetenskapliga eller historiska forskningsändamål och statistiska ändamål) inte är tillåten om den utförs med avseende på beslut som fattas med hänsyn till en viss registrerad eller sannolikt kommer att orsaka honom eller henne betydande skada eller lidande ([74]).

2.4.3 *Noggrannhet och uppgiftsminimering*

(45) Uppgifterna ska vara exakta och vid behov uppdaterade. De ska också vara adekvata, relevanta och inte överdrivet omfattande i förhållande till de ändamål som de behandlas för. I likhet med artikel 4.1 c, d och e i direktiv (EU) 2016/680 säkerställs dessa principer i avsnitten 37 och 38 i dataskyddslagen från 2018. Alla rimliga åtgärder måste vidtas för att se till att personuppgifter som är felaktiga ([75]) raderas eller rättas utan

([71]) *Guide to Law Enforcement Processing, "Conditions for sensitive processing"* (se fotnot 70).

([72]) Behandlingen utförs utan den registrerade personens samtycke när a) samtycke till behandlingen inte kan ges av den registrerade personen, b) den personuppgiftsansvariga rimligen inte kan förväntas erhålla den registrerades samtycke till behandlingen och c) behandlingen måste utföras utan den registrerades samtycke, eftersom erhållande av den registrerades samtycke skulle inverka menligt på det skydd som anges i stycke 1 a.

([73]) Se avsnitt 41.1 i dataskyddslagen från 2018.

([74]) Se avsnitt 41.2 i dataskyddslagen från 2018.

([75]) I avsnitt 205 i dataskyddslagen från 2018 definieras begreppet "oriktiga" som "felaktiga eller vilseledande" personuppgifter. Förenade kungarikets myndigheter har förklarat att det är typiskt att uppgifter som rör brottsutredningar ofta är ofullständiga men oavsett detta kan de vara korrekta.

dröjsmål ([76]), med hänsyn till de brottsbekämpande ändamål som de behandlas för ([77]) och för att se till att personuppgifter som är felaktiga, ofullständiga eller inaktuella inte överförs eller görs tillgängliga för något av de brottsbekämpande ändamålen ([78]).

(46) I likhet med artikel 7 i direktiv (EU) 2016/680 anges dessutom i Förenade kungarikets dataskyddssystem att personuppgifter som grundar sig på fakta så långt det är möjligt ska skiljas från personuppgifter som grundar sig på personliga bedömningar ([79]). Om det är relevant och så långt det är möjligt måste en tydlig åtskillnad göras mellan personuppgifter som rör olika kategorier av registrerade personer, till exempel misstänkta, personer som dömts för ett brott, brottsoffer och vittnen ([80]).

2.4.4 *Begränsad lagring*

(47) Enligt artikel 5 i direktiv (EU) 2016/680 bör uppgifter i princip inte lagras längre än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas. Enligt avsnitt 39 i dataskyddslagen från 2018 och i likhet med artikel 5 i det direktivet är det förbjudet att bevara personuppgifter som behandlas för något av de brottsbekämpande ändamålen längre än vad som är nödvändigt i förhållande till det ändamål för vilket de behandlas. Enligt Förenade kungarikets rättsordning måste lämpliga tidsfrister fastställas för den regelbundna översynen av behovet av fortsatt lagring av personuppgifter för något av de brottsbekämpande ändamålen. Ytterligare regler om praxis i samband med lagring av personuppgifter och tillämpliga tidsfrister har fastställts i relevant lagstiftning och vägledning om polisens befogenheter och funktion. I England och Wales ger t.ex. polisakademins (College of Policing's) *MOPI-Code of Practice*, tillsammans med *APP Guidance on the Management of Police Information*, en ram för att säkerställa en konsekvent riskbaserad process för lagring, granskning och bortskaffande av operativ polisinformation ([81]). Denna ram innehåller tydliga förväntningar på hur information ska skapas, delas, användas och hanteras inom och mellan enskilda polisstyrkor och andra organ ([82]). Polisen förväntas följa uppförandekoden och efterlevnaden kontrolleras av *Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services* ([83]).

(48) *Police Service of Northern Ireland* (PSNI) är enligt lag inte skyldig att följa *MoPI Code of Practice*. Den MoPI-ram som antogs 2011 kompletteras dock med en *PSNI Handbook* ([84]) som innehåller riktlinjer och förfaranden för hur *MoPI Code of Practice* tillämpas i Nordirland.

([76]) Avsnitt 38.1 b i dataskyddslagen från 2018.

([77]) Enligt *UK Explanatory Framework for Adequacy Discussion* "säkerställer detta att både de registrerades rättigheter och de brottsbekämpande organens operativa behov erkänns. Punkten ovan övervägdes noggrant under utarbetandet av dataskyddslagen eftersom det kan finnas specifika och begränsade operativa skäl till att uppgifter inte kan rättas. Det är sannolikt att detta kommer att vara fallet om de felaktiga personuppgifterna i fråga måste bevaras i sin ursprungliga form för bevisändamål" (se *UK Explanatory Framework for Adequacy Discussion section F: Law Enforcement*, s. 21, se fotnot 9).

([78]) Avsnitt 38.4 i dataskyddslagen från 2018. Enligt avsnitt 38.5 i dataskyddslagen från 2018 ska dessutom kvaliteten på personuppgifterna vid all överföring av personuppgifter kontrolleras innan de överförs eller görs tillgängliga, den nödvändiga information som gör det möjligt för mottagaren att bedöma i vilken utsträckninguppgifterna är riktiga, fullständiga och tillförlitliga och i vilken mån de är aktuella måste ingå och om det, när personuppgifterna har överförts, visar sig att uppgifterna var felaktiga eller att överföringen var olaglig ska mottagaren underrättas utan dröjsmål.

([79]) Avsnitt 38.2 i dataskyddslagen från 2018.

([80]) Avsnitt 38.3 i dataskyddslagen från 2018.

([81]) Denna ram säkerställer en konsekvent tillämpning av lagringen av de personuppgifter som erhållits. Omprövningsperioden beror på brotten som är uppdelade i följande 4 grupper: 1) Vissa frågor som rör skydd av allmänheten. 2) Andra sexuella våldsbrott och grova brott. 3) Alla andra brott. 4) Diverse. Mer information finns i *APP Guidance on the Management of Police Information* (se fotnot 26).

([82]) Enligt den information som lämnats av Förenade kungarikets myndigheter står det andra organisationer fritt att följa principerna för *MoPI Code of Practice* om de så önskar, till exempel antar *Her Majesty's Revenue and Customs* och *National Crime Agency* många av principerna i *MoPI Code of Practice* för att säkerställa konsekvens mellan olika brottsbekämpande myndigheter. I allmänhet kommer de flesta organisationer att ge sin personal specifika riktlinjer och vägledning för all personal om hur de ska hantera personuppgifter som en del av sin roll och som är skräddarsydda för den specifika organisationen. Detta skulle vanligtvis även omfatta obligatorisk utbildning.

([83]) *MoPI Code of Practice* utfärdades med stöd av de befogenheter som föreskrivs i polislagen från 1996 som gör det möjligt för polisakademin att utfärda riktlinjer för hur polisarbetet ska fungera effektivt. Varje uppförandekod som utfärdas enligt lagen måste godkännas av ministern och ska vara föremål för samråd med den nationella brottsmyndigheten innan den läggs fram i parlamentet. Enligt avsnitt 39A.7 i polislagen från 1996 ska polisen ta vederbörlig hänsyn till de lagar som utfärdats enligt polislagen från 1996.

([84]) *PSNI MOPI Handbook* kapitel 1–6.

(49) I Skottland förlitar sig polisstyrkorna på *Record Retention Standard Operating Procedure* (SOP) ([85]) som stöder *Police Service of Scotland Records Management Policy* ([86]). I standardrutinen fastställs särskilda regler för lagring av de register som innehas av polisen i Skottland.

(50) Utöver det övergripande kravet på granskning av register som gäller i hela Förenade kungariket ges ytterligare detaljer i lokala regler. För att ge några exempel, när det gäller England och Wales, innehåller *Police and Criminal Evidence Act*, ändrad genom *Protection of Freedom Act 2012* (PoFA), bestämmelser om lagring av fingeravtryck och DNA-profiler samt ett särskilt system för personer som inte dömts ([87]). PoFA inrättade också befattningen som *Commissioner for the Retention and Use of Biometric Material* (*Biometrics Commissioner*) ([88]). Särskilda regler för häktningsbilder finns i 2017 års översyn av häktningsbilder ([89]). När det gäller Skottland innehåller *Criminal Procedure (Scotland) Act 1995* regler för erhållande och lagring av fingeravtryck och biologiska prover ([90]). Liksom i England och Wales reglerar lagstiftningen lagring av biometriska uppgifter i olika fall ([91]).

2.4.5 *Datasäkerhet*

(51) Personuppgifter ska behandlas på ett sätt som garanterar deras säkerhet, inbegripet skydd mot obehörig eller otillåten behandling och mot oavsiktlig förlust, förstörelse eller skada. I detta syfte ska offentliga myndigheter vidta lämpliga tekniska eller organisatoriska åtgärder för att skydda personuppgifter från eventuella hot. Dessa åtgärder måste bedömas med beaktande av den aktuella kunskapsnivån och därmed sammanhängande kostnader.

(52) Dessa principer återspeglas i avsnitt 40 i dataskyddslagen från 2018 enligt vilket personuppgifter som behandlas för något av de brottsbekämpande ändamålen, i likhet med artikel 4.1 f i direktiv (EU) 2016/680, måste behandlas på ett sätt som garanterar lämplig säkerhet för personuppgifterna med hjälp av lämpliga tekniska eller organisatoriska åtgärder. Detta inbegriper att skydda uppgifterna mot otillåten eller olaglig behandling och mot oavsiktlig förlust,

([85]) *Record Retention Standard Operating Procedure* (SOP) finns på följande länk: https://www.scotland.police.uk/spa-media/nhobty5i/record-retention-sop.pdf.

([86]) För mer information om dokumenthantering, se information om *National Records of Scotland* på följande länk: https://www.nrscotland.gov.uk/record-keeping/records-management.

([87]) Lagringstiderna varierar beroende på om en person har dömts eller inte (avsnitten 63I–63KI i Pace 1984). Till exempel när det gäller en vuxen som dömts för ett registreringsbart brott kan hans eller hennes fingeravtryck och DNA-profil behållas på obestämd tid (avsnitt 63I.2 i Pace 1984) medan lagringen är tidsbegränsad om den dömda personen är under 18 år, brottet är ett ”ringa” registrerbart brott och personen inte tidigare har dömts (avsnitt 63K i Pace 1984). Lagring när det gäller en person som gripits eller åtalats men inte dömts är tidsbegränsad till tre år (avsnitt 63F i Pace 1984). Förlängningen av denna lagringstid måste godkännas av en rättslig myndighet (avsnitt 63F 7 i Pace 1984). När det gäller personer som gripits eller åtalats men inte dömts för ringa brott är det inte möjligt att behålla dem (avsnitt 63D och 63H i Pace 1984).

([88]) I avsnitt 20 i PoFA 2012 fastställs Biometrics Commissioner's ståndpunkt. Biometrics Commissioner avgör bland annat om polisen får behålla DNA-profiler och fingeravtryck från personer som gripits men inte åtalats för ett kvalificerat brott (avsnitt 63G i Pace 1984). Dessutom har Biometrics Commissioner ett allmänt ansvar för att se över lagringen och användningen av DNA och fingeravtryck och lagringen av nationella säkerhetsskäl (avsnitt 20.2 i POFA 2012). Biometrics Commissioner utses enligt *Code for Public Appointments* (finns på följande länk: Governance Code for Public Appointments - GOV.UK (www.gov.uk)). Av villkoren för förordnandet framgår tydligt att kommissionären endast kan avsättas av inrikesministern under snävt definierade omständigheter, exempelvis om vederbörande inte fullgör sina förpliktelser under en tremånadersperiod, döms för ett brott eller inte iakttar villkoren för förordnandet.

([89]) Översyn av användning och lagring av häktningsbilder finns på följande länk: https://www.gov.uk/government/publications/custody-images-review-of-their-use-and-retention.

([90]) Avsnitt 18 och följande i *Criminal Procedure (Scotland) Act 1995*.

([91]) Lagringstiden varierar beroende på om personen har dömts (avsnitt 18(3) i Criminal Procedure (Scotland) Act 1995) eller om personen är minderårig. I det senare fallet är lagringstiden 3 år från domen i målet vid barnets förhandling (avsnitt 18E.8 i *Criminal Procedure (Scotland) Act 1995*). Uppgifter om personer som gripits men inte dömts kan inte bibehållas (avsnitt 18.3 i *Criminal Procedure (Scotland) Act 1995*) utom i särskilda fall och beroende på brottets svårhetsgrad (avsnitt 18A i *Criminal Procedure (Scotland) Act 1995*). *Scottish Biometrics Commissioner Act 2020* (se https://www.legislation.gov.uk/asp/2020/8/contents) skapar en ståndpunkt för den skotska Biometrics Commissioner som måste utarbeta och se över uppförandekoder (godkända av Skottlands parlament) om insamling, lagring, användning och förstöring av biometriska uppgifter för straffrättsliga och polisiära ändamål (avsnitt 7 i *Scottish Biometrics Commissioner Act 2020*).

förstöring eller skada ([92]). I avsnitt 66 i dataskyddslagen från 2018 anges vidare att varje registeransvarig och personuppgiftsbiträde ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig med hänsyn till de risker som behandlingen av personuppgifter medför. Enligt de förklarande anmärkningarna ska den personuppgiftsansvariga utvärdera riskerna och vidta lämpliga säkerhetsåtgärder på grundval av denna utvärdering, till exempel kryptering eller särskilda säkerhetsnivåer för personal som behandlar uppgifterna ([93]). Utvärderingen måste till exempel dessutom ta hänsyn till vilken typ av uppgifter som behandlas och andra relevanta faktorer eller omständigheter som kan påverka behandlingens säkerhet.

(53) Det system som reglerar efterlevnaden av principerna för datasäkerhet är mycket likt det system som fastställs i artiklarna 29–31 i direktiv (EU) 2016/680. I synnerhet vid ett personuppgiftsbrott i samband med personuppgifter för vilka den personuppgiftsansvariga är ansvarig, enligt avsnitt 67(1) i dataskyddsmyndigheten 2018, ska den personuppgiftsansvariga utan onödigt dröjsmål och om möjligt inom 72 timmar efter att ha fått kännedom om incidenten anmäla personuppgiftsbrottet till *Information Commissioner* ([94]). Anmälningsskyldigheten gäller inte om personuppgiftsincidenten sannolikt inte kommer att leda till en risk för enskildas rättigheter och friheter ([95]). Den personuppgiftsansvariga ska dokumentera fakta om ett personuppgiftsbrott, dess effekter och korrigerande åtgärder som vidtagits på ett sätt som gör det möjligt för *Information Commissioner* att kontrollera efterlevnaden av dataskyddsmyndigheten ([96]). Om ett personuppgiftsbiträde får kännedom om ett säkerhetsbrott ska det utan onödigt dröjsmål underrätta den personuppgiftsansvariga om detta ([97]).

(54) Enligt avsnitt 68.1 i dataskyddslagen från 2018 ska den personuppgiftsansvariga utan onödigt dröjsmål informera den registrerade om brottet om ett personuppgiftsbrott sannolikt medför en hög risk för enskildas rättigheter och friheter ([98]). Meddelandet måste innehålla samma information som den anmälan till *Information Commissioner* som beskrivs i skäl (53). Denna skyldighet gäller inte om den personuppgiftsansvariga har genomfört lämpliga tekniska och organisatoriska skyddsåtgärder som tillämpades på de personuppgifter som berördes av brottet. Det gäller inte heller om den personuppgiftsansvariga har vidtagit efterföljande åtgärder som säkerställer att den höga risken för de registrerade personernas rättigheter och friheter sannolikt inte längre kommer att förverkligas. Slutligen är den personuppgiftsansvariga inte skyldig att underrätta den registrerade om detta skulle innebära en oproportionerligt stor ansträngning ([99]). I så fall måste informationen göras tillgänglig för den registrerade på ett annat lika effektivt sätt, till exempel genom offentlig kommunikation ([100]). Om den personuppgiftsansvariga inte har informerat den registrerade om incidenten kan *Information Commissioner*, efter att ha underrättats i enlighet med avsnitt 67 i dataskyddslagen och efter att ha övervägt sannolikheten för att det brott som leder till en hög risk kan kräva att den personuppgiftsansvariga underrättar den registrerade om brottet ([101]).

([92]) I enlighet med de förklarande anmärkningarna till dataskyddsmyndigheten 2018 (se fotnot 45) ska den personuppgiftsansvariga särskilt utforma och organisera säkerheten så att den är lämpad för karaktären hos de personuppgifter som den personuppgiftsansvariga innehar och den skada som kan uppstå till följd av en säkerhetsöverträdelse, vara tydlig om vem i deras organisation som ansvarar för informationssäkerheten, se till att de har rätt fysisk och teknisk säkerhet, backas upp av robusta strategier och förfaranden samt pålitlig och välutbildad personal och vara redo att reagera snabbt och effektivt på alla säkerhetsöverträdelser.

([93]) Punkt 221 i de förklarande anmärkningarna till dataskyddsmyndigheten 2018 (se fotnot 45).

([94]) I avsnitt 67.4 i dataskyddslagen från 2018 föreskrivs att anmälan ska innehålla en beskrivning av personuppgiftsbrottets art (inklusive, när så är möjligt, de kategorier och det ungefärliga antalet registrerade personer som berörs samt de kategorier och det ungefärliga antal personuppgifter som berörs), namn och kontaktuppgifter för en kontaktpunkt, en beskrivning av de sannolika konsekvenserna av personuppgiftsbrottet och en beskrivning av de åtgärder som den personuppgiftsansvariga har vidtagit eller föreslagit för att hantera personuppgiftsbrottet (inbegripet, i förekommande fall, åtgärder för att mildra dess eventuella negativa effekter).

([95]) Avsnitt 67.2 i dataskyddslagen från 2018.

([96]) Avsnitt 67.6 i dataskyddslagen från 2018.

([97]) Avsnitt 67.9 i dataskyddslagen från 2018.

([98]) Enligt avsnitt 68.7 i dataskyddslagen från 2018 får den personuppgiftsansvariga helt eller delvis begränsa tillhandahållandet av information till den registrerade i den utsträckning och så länge begränsningen, med beaktande av den registrerades grundläggande rättigheter och berättigade intressen, är en nödvändig och proportionell åtgärd för att a) undvika att hindra en officiell eller rättslig undersökning, utredning eller dito förfarande, b) att undvika att inverka menligt på förebyggande, upptäckt, utredning eller lagföring av brott eller verkställighet av straffrättsliga påföljder, c) att skydda den allmänna säkerheten, d) att skydda den nationella säkerheten och e) att skydda andras fri- och rättigheter.

([99]) Avsnitt 68.3 i dataskyddslagen från 2018.

([100]) Avsnitt 68.5 i dataskyddslagen från 2018.

([101]) Avsnitt 68.6 i dataskyddslagen från 2018, med förbehåll för den begränsning som föreskrivs i avsnitt 68.8 i dataskyddslagen från 2018.

2.4.6 *Insyn*

(55) De registrerade måste informeras om huvuddragen i behandlingen av sina personuppgifter. Denna princip om skydd av personuppgifter återspeglas i avsnitt 44 i dataskyddslagen från 2018, där det, i likhet med artikel 13 i direktiv (EU) 2016/680, föreskrivs att den personuppgiftsansvariga har en allmän skyldighet att ge de registrerade tillgång till information om behandlingen av deras personuppgifter (antingen genom att göra informationen allmänt tillgänglig för allmänheten eller på annat sätt) ([102]). Den information som ska göras tillgänglig omfattar a) den personuppgiftsansvarigas identitet och kontaktuppgifter, b) i tillämpliga fall, dataskyddsombudets kontaktuppgifter, c) de ändamål för vilka den personuppgiftsansvariga behandlar personuppgifter, d) de registrerades rätt att av den personuppgiftsansvariga begära tillgång till personuppgifter, rättelse av personuppgifter och radering av personuppgifter eller begränsning av behandlingen av dem och e) förekomsten av rätten att lämna in ett klagomål till *Information Commissioner* samt hans eller hennes kontaktuppgifter ([103]).

(56) Den personuppgiftsansvariga måste också, i särskilda fall för att göra det möjligt för den registrerade personen att utöva sina rättigheter enligt dataskyddslagen från 2018 (till exempel när de personuppgifter som behandlas har samlats in utan den registrerade personens vetskap) och ge den registrerade information om a) den rättsliga grunden för behandlingen, b) information om den period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, om de kriterier som används för att fastställa denna period, c) i tillämpliga fall, information om kategorier av mottagare av personuppgifterna (inklusive mottagare i tredjeländer eller internationella organisationer) och d) den ytterligare information som är nödvändig för att den registrerade personen ska kunna utöva sina rättigheter enligt del 3 i dataskyddslagen från 2018 ([104]).

2.4.7 *Individuella rättigheter*

(57) De registrerade måste beviljas ett antal rättigheter som kan verkställas. Kapitel 3 i del 3 i dataskyddslagen från 2018 ger enskilda personer rättigheter till tillgång, rättelse, radering och begränsning ([105]), vilka är jämförbara med dem som föreskrivs i kapitel 3 i direktiv (EU) 2016/680.

(58) Rätten till tillträde anges i avsnitt 45 i dataskyddslagen från 2018. För det första har en enskild rätt att få en bekräftelse från den personuppgiftsansvariga om huruvida hans eller hennes personuppgifter behandlas eller inte ([106]). För det andra har den registrerade personen, om personuppgifterna behandlas, rätt att få tillgång till dessa uppgifter och få följande information om behandlingen: a) Ändamålen med och de rättsliga grunderna för behandlingen. b) De kategorier av uppgifter som berörs. c) Den mottagare till vilken uppgifterna har lämnats ut. d) Den period under vilken personuppgifterna ska lagras. e) Den registrerade personens rätt till rättelse och radering av personuppgifter. f) Rätt att lämna in klagomål. g) All information om de berörda personuppgifternas ursprung ([107]).

(59) Enligt avsnitt 46 i dataskyddslagen från 2018 har den registrerade rätt att kräva att den personuppgiftsansvariga rättar felaktiga personuppgifter som rör honom eller henne. Den personuppgiftsansvariga ska rätta (eller komplettera dem om uppgifterna är felaktiga på grund av att de är ofullständiga) uppgifterna utan onödigt dröjsmål. Om personuppgifterna måste bevaras för bevisändamål måste den personuppgiftsansvariga (i stället för att rätta personuppgifterna) begränsa behandlingen av dem ([108]).

([102]) I *Guide to Law Enforcement Processing* ges följande exempel:"Ni har ett allmänt meddelande meddelande om skydd av personuppgifter på er webbplats som innehåller grundläggande information om organisationen, syftet med behandlingen av personuppgifter, den registrerade personens rättigheter och deras rätt att klaga hos Information Commissioner. Du har fått information om att en person var närvarande när ett brott ägde rum. Vid den första intervjun av denna person måste du lämna den allmänna informationen och ytterligare styrkande information för att de ska kunna utöva sina rättigheter. Du kan bara begränsa den information om rättvis behandling som du lämnar om den kommer att inverka negativt på den undersökning du utför (*Guide to Law Enforcement Processing, "What information should we supply to an individual?"* finns på följande länk: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-to-be-informed/#ib3).

([103]) I *Guide to Law Enforcement Processing* anges att den information som lämnas om behandlingen av personuppgifter ska vara kortfattad, begriplig och lättillgänglig, vara skriven med ett klart och tydligt språk så att den anpassas till behoven hos utsatta personer, t.ex. barn och gratis (*Guide to Law Enforcement Processing, "How should we provide this information?"* finns på följande länk: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-to-be-informed/#ib1).

([104]) Avsnitt 44.2 i dataskyddslagen från 2018.

([105]) En detaljerad analys av försökspersonernas rättigheter finns på *Guide to Law Enforcement Processing on individual rights* finns på följande länk: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/

([106]) Avsnitt 45.1 i dataskyddslagen från 2018.

([107]) Avsnitt 45.2 i dataskyddslagen från 2018.

([108]) Avsnitt 46.4 i dataskyddslagen från 2018.

(60) Enligt avsnitt 47 i dataskyddslagen från 2018 har enskilda rätt till radering och begränsning av behandlingen. Den personuppgiftsansvariga ska ([109]) radera personuppgifter utan onödigt dröjsmål om behandlingen av personuppgifterna skulle strida mot någon av dataskyddsprinciperna, de rättsliga grunderna för behandlingen eller skyddsåtgärderna i samband med arkivering och känslig behandling. Den personuppgiftsansvariga måste också radera uppgifterna om de har en rättslig skyldighet att göra det. Om personuppgifterna måste bevaras för bevisändamål måste den personuppgiftsansvariga (i stället för att radera personuppgifterna) begränsa behandlingen av dem ([110]). Den personuppgiftsansvariga måste begränsa behandlingen av personuppgifter om den registrerade personen bestrider att personuppgifterna är korrekta och det är inte möjligt att fastställa om de är korrekta eller inte ([111]).

(61) Om en registrerad person begär rättelse eller radering av personuppgifter eller begränsning av behandlingen av dem måste den personuppgiftsansvariga skriftligen informera den registrerade om huruvida begäran har beviljats och om den har avslagits måste han eller hon informera den registrerade personen om skälen till avslaget och vilka möjligheter till rättslig prövning som finns (den registrerades rätt att vända sig till *Information Commissioner* för att undersöka om begränsningen har tillämpats lagligt, rätt att lämna in ett klagomål till *Information Commissioner* och rätt att ansöka om ett föreläggande om efterlevnad hos en domstol) ([112]).

(62) Om den personuppgiftsansvariga rättar personuppgifter som mottagits från en annan behörig myndighet ska den underrätta den andra myndigheten ([113]). Om den personuppgiftsansvariga korrigerar, raderar eller begränsar behandlingen av personuppgifter som har lämnats ut av den personuppgiftsansvariga ska den personuppgiftsansvariga underrätta mottagarna och mottagarna ska på motsvarande sätt korrigera, radera eller begränsa behandlingen av personuppgifterna (i den mån de behåller ansvaret för behandlingen) ([114]).

(63) Dessutom har den registrerade personen rätt att utan onödigt dröjsmål informeras av den personuppgiftsansvariga om ett personuppgiftsbrott när detta sannolikt kommer att leda till en hög risk för den enskilda personens rättigheter och friheter ([115]).

(64) När det gäller alla dessa rättigheter för den registrerade personen och i likhet med vad som föreskrivs i artikel 12 i direktiv (EU) 2016/680 är den personuppgiftsansvariga skyldig att se till att all information som den registrerade får lämnas i en koncis, begriplig och lättillgänglig form ([116]) och, om möjligt, tillhandahållas i samma form som begäran ([117]). Den personuppgiftsansvariga måste tillmötesgå en begäran från den registrerade utan onödigt dröjsmål eller under alla omständigheter före utgången av en period på en månad från begäran ([118]). Om den personuppgiftsansvariga har rimliga skäl att betvivla en persons identitet får han eller hon begära ytterligare information och skjuta upp behandlingen av begäran till dess att identiteten har fastställts. Den personuppgiftsansvariga kan kräva en rimlig avgift eller vägra att agera om han eller hon anser att begäran är uppenbart ogrundad ([119]). ICO har gett vägledning om när en begäran anses vara uppenbart ogrundad eller orimlig och när en avgift kan begäras ([120]).

(65) Enligt avsnitt 53.4 i dataskyddslagen från 2018 kan ministern dessutom genom förordningar fastställa maximibeloppet för en avgift.

([109]) En registrerad person kan begära att den personuppgiftsansvariga raderar personuppgifter eller begränsar behandlingen av dem (men den personuppgiftsansvarigas skyldigheter att radera uppgifterna eller begränsa behandlingen av dem gäller oavsett om en sådan begäran görs eller inte).

([110]) Avsnitt 46.4 och 47.2 i dataskyddslagen från 2018.

([111]) Avsnitt 47.3 i dataskyddslagen från 2018.

([112]) Avsnitt 48.1 i dataskyddslagen från 2018.

([113]) Avsnitt 48.7 i dataskyddslagen från 2018.

([114]) Avsnitt 48.9 i dataskyddslagen från 2018.

([115]) Avsnitt 68 i dataskyddslagen från 2018.

([116]) Avsnitt 52.1 i dataskyddslagen från 2018.

([117]) Avsnitt 52.3 i dataskyddslagen från 2018.

([118]) I avsnitt 54 i dataskyddslagen från 2018 definieras vad som avses med ”tillämplig tidsperiod”, dvs. den period på 1 månad, eller den längre period som kan anges i förordningar, med början vid den relevanta tidpunkten (när den personuppgiftsansvariga mottar begäran i fråga, när den personuppgiftsansvariga mottar den information (i förekommande fall) som begärs i samband med en begäran enligt avsnitt 52.4 i dataskyddslagen eller när den avgift (i förekommande fall) som tas ut i samband med begäran enligt avsnitt 53 i dataskyddslagen betalas.

([119]) Avsnitt 53.1 i dataskyddslagen från 2018.

([120]) Enligt ICO:s vägledning kan en registeransvarig besluta att ta ut en avgift av en registrerad person om hans eller hennes begäran är uppenbart ogrundad eller orimlig men ändå väljer att besvara den. Avgiften ska vara rimlig och kunna motivera kostnaden. *Guide to Law Enforcement Processing ”Manifestly unfounded and excessive requests”* finns på följande länk: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/manifestly-unfounded-and-excessive-requests/

2.4.7.1. Begränsningar av den registrerade personens rättigheter och transparenskrav

(66) En behörig myndighet kan under vissa omständigheter begränsa vissa av den registrerade personens rättigheter enligt följande: Rätten att få tillgång till ([121]), bli informerad ([122]) om ett personuppgiftsbrott ([123]) och att informeras om orsaken till att en begäran om rättelse eller radering har avslagits ([124]). I likhet med systemet i kapitel III i direktiv (EU) 2016/680 kan den behöriga myndigheten endast tillämpa begränsningen om den med beaktande av den registrerade personens grundläggande rättigheter och berättigade intressen är nödvändig och proportionell i förhållande till a) att undvika att hindra en officiell eller rättslig undersökning, utredning eller dito förfarande, b) att undvika att inverka menligt på förebyggande, upptäckt, utredning eller lagföring av brott eller verkställighet av straffrättsliga påföljder, c) att skydda den allmänna säkerheten, d) att skydda den nationella säkerheten och e) att skydda andras fri- och rättigheter.

(67) ICO har gett vägledning om tillämpningen av dessa begränsningar. Enligt denna vägledning måste personuppgiftsansvariga göra en analys från fall till fall för att göra en avvägning mellan den enskildas rättigheter och den skada som ett utlämnande skulle orsaka. I synnerhet måste de motivera eventuella begränsningar som tillämpas när de är nödvändiga och proportionerliga och får endast begränsa vad som föreskrivs om det skulle inverka menligt på ovannämnda syften ([125]).

(68) Det finns också ett antal andra riktlinjer från behöriga myndigheter som ger detaljerad information om alla aspekter av dataskyddslagstiftningen, inbegripet tillämpningen av begränsningarna av de registrerades rättigheter ([126]). När det till exempel gäller avsnitt 45.4 anges följande i *Data Protection Manual of the National Police Chief's Counsel*: "Det är viktigt att notera att begränsningarna endast kan tillämpas i den mån det är nödvändigt och endast kan tillämpas så länge det är nödvändigt. En generell tillämpning av begränsningen till en sökandes samtliga personuppgifter eller en permanent tillämpning av begränsningen är således inte tillåten. När det gäller den sistnämnda punkten är det ofta så att personuppgifter som samlas in utan kännedom hos den registrerade personen som är misstänkt i en utredning inledningsvis måste skyddas från att lämnas ut till dem för att inte skada utredningen medan utredningen pågår men vid ett senare tillfälle skulle ett utlämnande inte medföra någon skada om personuppgifterna hade lämnats ut till den enskilda personen under intervjun. Polisen måste anta förfaranden som säkerställer att tillämpningen av dessa restriktioner endast sker i den utsträckning som krävs och endast under den tid som krävs ([127])." Denna vägledning ger också exempel på när var och en av begränsningarna sannolikt kommer att tillämpas ([128]).

(69) När det gäller möjligheten att begränsa någon av de ovannämnda rättigheterna till skydd för "nationell säkerhet" kan en registeransvarig ansöka om ett intyg som undertecknats av en minister eller justitieministern (eller Advocate General for Scotland) som intygar att en begränsning av sådana rättigheter är en nödvändig och proportionerlig åtgärd för att skydda den nationella säkerheten ([129]). Förenade kungarikets regering har utfärdat riktlinjer om nationella säkerhetscertifikat enligt dataskyddslagen från 2018, där det särskilt framhålls att varje begränsning av registrerades rättigheter för att skydda den nationella säkerheten måste vara proportionerlig och nödvändig ([130]) (för mer information om de nationella säkerhetsintygen, se skälen (131)–(134)).

([121]) Avsnitt 45.4 i dataskyddslagen från 2018.
([122]) Avsnitt 44.4 i dataskyddslagen från 2018.
([123]) Avsnitt 68.7 i dataskyddslagen från 2018.
([124]) Avsnitt 48.3 i dataskyddslagen från 2018.
([125]) Se till exempel *Guide to Law Enforcement Processing* om rätten till tillgång, som finns på följande webbplats:https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-of-access/#ib8
([126]) Se t.ex. *Data Protection Manual for Police Data Protection Professional* som utfärdats av National Police Chief Counsel (se fotnot 27) eller vägledningen från Serious Fraud Office, som finns på följande länk: https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/data-protection/
([127]) Data protection Manual of the National Police Chief Counsel, s. 140 (se fotnot 27).
([128]) I Data protection Manual of the National Police Chief Counsel föreskrivs att "undvika att hindra en officiell eller rättslig undersökning, utredning eller förfarande" sannolikt är relevant för personuppgifter som behandlas i samband med undersökningar, familjerättsliga förfaranden, utredningar om interna disciplinärenden som inte är straffbelagda och undersökningar som oberoende utredning av sexuella övergrepp mot barn medan "skydda andras fri- och rättigheter" är relevant för personuppgifter som även skulle gälla andra personer samt den sökande" (Data protection Manual of the National Police Chief Counsel, s. 140, se fotnot 27).
([129]) Avsnitt 79 i dataskyddslagen från 2018.
([130]) Den brittiska regeringens vägledning om nationella säkerhetscertifikat finns på följande länk: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf.

(70) Om en begränsning av en registrerad persons rättigheter är tillämplig ska den behöriga myndigheten dessutom utan onödigt dröjsmål informera den registrerade personen om att deras rättigheter har begränsats, om skälen till begränsningen och om vilka möjligheter till prövning som står till buds, såvida inte ett tillhandahållande av informationen skulle undergräva skälet till att tillämpa begränsningen ([131]). Som ytterligare ett skydd mot missbruk av begränsningar måste den personuppgiftsansvariga registrera skälen till att begränsa informationen och på begäran göra registret tillgängligt för *Information Commissioner* ([132]).

(71) Om den personuppgiftsansvariga vägrar att tillhandahålla ytterligare information om öppenhet eller tillgång eller avslår en begäran om rättelse, radering eller begränsning av behandling, kan den enskilda begära att *Information Commissioner* utreder om den personuppgiftsansvariga har använt begränsningen på ett lagligt sätt ([133]). Den berörda personen kan också lämna in ett klagomål till *Information Commissioner* eller begära att en domstol ålägger den personuppgiftsansvariga att tillmötesgå begäran ([134]).

2.4.7.2. Automatiserat beslutsfattande

(72) Avsnitten 49 och 50 i dataskyddslagen från 2018 omfattar rättigheterna i samband med automatiserat beslutsfattande respektive de skyddsåtgärder som ska tillämpas ([135]). I likhet med vad som föreskrivs i artikel 11 i direktiv (EU) 2016/680, är det endast om det krävs eller är tillåtet enligt lag som den personuppgiftsansvariga kan fatta ett viktigt beslut enbart på grundval av automatiserad behandling av personuppgifter ([136]). Ett beslut är betydande om det skulle få negativa rättsliga följder för den registrerade eller i betydande grad påverka honom eller henne ([137]).

(73) Om den personuppgiftsansvariga enligt lag är skyldig eller bemyndigad att fatta ett viktigt beslut anges det i avsnitt 50 i dataskyddslagen från 2018 vilka skyddsåtgärder som ska gälla för ett sådant beslut (vilket definieras som ett kvalificerat betydande beslut). Den personuppgiftsansvariga ska så snart det rimligen är praktiskt möjligt underrätta den registrerade personen om att ett sådant beslut har fattats. Den registrerade personen kan därefter inom en månad begära att den personuppgiftsansvariga omprövar beslutet eller fattar ett nytt beslut som inte enbart grundar sig på automatiserad behandling. Den personuppgiftsansvariga ska behandla begäran och informera den registrerade om resultatet av behandlingen. Dataskyddslagen från 2018 ger ministern befogenhet att anta bestämmelser om ytterligare skyddsåtgärder ([138]). Inga sådana förordningar har ännu antagits.

2.4.8 *Vidare överföringar*

(74) Skyddsnivån för personuppgifter som överförs från en brottsbekämpande myndighet i en medlemsstat till en brottsbekämpande myndighet i Förenade kungariket får inte undergrävas av en ytterligare överföring av sådana uppgifter till mottagare i ett tredjeland. Sådana ”vidareöverföringar” som ur synvinkeln för en brottsbekämpande myndighet i Förenade kungariket utgör internationella överföringar från Förenade kungariket bör endast tillåtas om den ytterligare mottagaren utanför Förenade kungariket själv omfattas av regler som säkerställer en skyddsnivå som liknar den som garanteras i Förenade kungarikets rättsordning.

([131]) Avsnitten 44.5 och 44.6: Avsnitten 45.5 och 45.6, avsnitt 48.4 i dataskyddslagen från 2018.
([132]) Avsnitt 44.7, avsnitt 45.7, avsnitt 48.6 i dataskyddslagen från 2018.
([133]) Avsnitt 51 i dataskyddslagen från 2018.
([134]) Avsnitt 167 i dataskyddslagen från 2018.
([135]) När det gäller omfattningen av den automatiserade behandlingen anges följande i de förklarande anmärkningarna till dataskyddslagen från 2018: ”Dessa bestämmelser rör helt automatiserat beslutsfattande och inte automatisk behandling. Automatisk behandling (inbegripet profilering) är när en åtgärd utförs på uppgifter utan att det behövs någon mänsklig medverkan. Den används regelbundet inom brottsbekämpande myndigheter för att filtrera stora datamängder till hanterbara mängder som en mänsklig aktör sedan kan använda. Automatiserat beslutsfattande är en form av automatiserad behandling och kräver att det slutliga beslutet fattas utan mänsklig inblandning.” (De förklarande anmärkningarna till dataskyddslagen, punkt 204, se fotnot 45).
([136]) Förutom det skydd som ges enligt dataskyddslagen innehåller den rättsliga ramen in Förenade kungariket andra lagstadgade begränsningar som är tillämpliga på brottsbekämpande organ och skulle förhindra automatiserad behandling (inklusive profilering) om den skulle leda till olaglig diskriminering. Genom *The Human Rights Act 1998* införlivas de rättigheter som ges i Europakonventionen i Förenade kungarikets lagstiftning, inbegripet diskrimineringsförbudet i artikel 14 i konventionen. Vidare förbjuder *Equality Act 2010* diskriminering av personer med skyddade egenskaper (kön, ras, funktionsnedsättning osv.).
([137]) Avsnitt 49.2 i dataskyddslagen från 2018.
([138]) Avsnitt 50.4 i dataskyddslagen från 2018.

(75) Förenade kungarikets ordning för internationella överföringar regleras i del 3 kapitel 5 i dataskyddslagen från 2018 ([139]) och återspeglar tillvägagångssättet i kapitel V i direktiv (EU) 2016/680. För att överföra personuppgifter till ett tredjeland måste en behörig myndighet uppfylla följande tre villkor: a) Överföringen måste vara nödvändig för brottsbekämpning. b) Överlåtelsen ska grunda sig på i) en förordning om adekvat skyddsnivå med avseende på tredjelandet, ii) om den inte grundar sig på en förordning om adekvat skyddsnivå, förekomsten av lämpliga skyddsåtgärder eller iii) om den inte grundar sig på ett beslut om adekvat skyddsnivå eller lämpliga skyddsåtgärder, måste den grundas på särskilda omständigheter. c) Mottagaren av överföringen ska vara i) en relevant myndighet (dvs. motsvarigheten till en behörig myndighet) i tredjelandet, ii) en ”relevant internationell organisation”, t.ex. ett internationellt organ som utför uppgifter som motsvarar något av de brottsbekämpande ändamålen eller iii) en person som inte är en relevant myndighet men endast om överföringen är absolut nödvändig för att fullgöra något av de brottsbekämpande ändamålen, det inte finns några grundläggande rättigheter och friheter för den registrerade personen som väger tyngre än det allmänintresse som kräver överföringen, en överföring av personuppgifterna till en relevant myndighet i tredjelandet skulle vara ineffektiv eller olämplig och mottagaren informeras om de ändamål för vilka uppgifterna får behandlas ([140]).

(76) Bestämmelser om adekvat skyddsnivå med avseende på ett tredjeland, ett territorium eller en sektor inom ett tredjeland, en internationell organisation eller en beskrivning ([141]) av ett sådant land, territorium, sektor eller organisation antas av ministern. När det gäller den standard som ska uppfyllas måste ministern bedöma om ett sådant territorium/en sådan sektor/organisation säkerställer en adekvat skyddsnivå för personuppgifter. I avsnitt 74A.4 i dataskyddslagen från 2018 anges att ministern i detta syfte ska beakta ett antal faktorer som återspeglar dem som anges i artikel 36 i direktiv (EU) 2016/680 ([142]). Sedan övergångsperiodens slut utgör del 3 i dataskyddslagen från 2018 ”inhemsk EU-lagstiftning” som, enligt förklaringen, kommer att tolkas av domstolar i Förenade kungariket i enlighet med relevant rättspraxis från domstolen från tiden före Förenade kungarikets utträde ur unionen och allmänna principer i unionsrätten eftersom de hade verkan omedelbart före övergångsperiodens utgång. Detta inbegriper den ”väsentliga likvärdighetsstandard” som därmed kommer att gälla för de bedömningar av adekvat skyddsnivå som utförs av Förenade kungarikets myndigheter.

(77) När det gäller förfarandet omfattas förordningarna av de ”allmänna” förfarandekrav som anges i avsnitt 182 i dataskyddslagen från 2018. Enligt detta förfarande måste ministern samråda med *Information Commissioner* när han

([139]) Denna nya ram blev till i slutet av övergångsperioden, inklusive ministerns befogenhet att utfärda föreskrifter om adekvat skyddsnivå. I DPPEC-förordningarna (särskilt punkterna 10–12 i tillägg 21 som dessa förordningar för in i dataskyddslagen från 2018) föreskrivs emellertid att vissa överföringar av personuppgifter under och efter övergångsperiodens utgång ska behandlas som om de grundar sig på förordningar om adekvat skyddsnivå. Dessa överföringar omfattar överföringar till tredjeländer som är föremål för ett EU-beslut om adekvat skyddsnivå vid övergångsperiodens utgång och till EU-medlemsstater, Eftastater och territoriet Gibraltar genom deras tillämpning av direktivet om brottsbekämpning på behandling av uppgifter inom brottsbekämpning (Eftastaterna tillämpar direktiv (EU) 2016/680 på grund av sina skyldigheter enligt Schengenregelverket). Detta innebär att överföringarna till dessa länder kan fortsätta i slutet av övergångsperioden precis som före EU:s utträde. Efter övergångsperiodens utgång måste ministern inom fyra år göra en översyn av slutsatserna om adekvat skyddsnivå.

([140]) Avsnitt 73 och 77 i dataskyddslagen från 2018.

([141]) Förenade kungarikets myndigheter har förklarat att beskrivningen av ett land eller en internationell organisation avser en situation där det skulle vara nödvändigt att göra ett specifikt och partiellt fastställande av adekvat skyddsnivå med fokuserade begränsningar (t.ex. en förordning om adekvat skyddsnivå som endast avser vissa typer av uppgiftsöverföringar).

([142]) Se avsnitt 74A.4 i dataskyddslagen från 2018, där det föreskrivs att vid bedömningen av om skyddsnivån är adekvat måste ”ministern särskilt beakta a) rättsstatsprincipen, respekten för de mänskliga rättigheterna och de grundläggande friheterna, relevant lagstiftning, både allmän och sektoriell, inbegripet allmän säkerhet, försvar, nationell säkerhet och straffrätt och offentliga myndigheters tillgång till personuppgifter samt genomförande av sådan lagstiftning, regler om dataskydd, yrkesregler och säkerhetsåtgärder, inklusive regler för en vidareöverföring av personuppgifter till ett tredjeland eller en internationell organisation som följs i detta land eller i denna internationella organisation, rättspraxis samt effektiv och rättigheter som kan verkställas för den registrerade samt effektiv administrativ och rättslig prövning för registrerade vars personuppgifter överförs, b) det ska finnas en eller flera fungerande oberoende tillsynsmyndigheter i tredjelandet eller som en internationell organisation lyder under med ansvar för att säkerställa och verkställa efterlevnaden av dataskyddsreglerna inklusive adekvata befogenheter för verkställande, för att assistera och råda registrerade när det gäller att utöva sina rättigheter och för att samarbeta med Commissioner och c) de internationella åtaganden som tredjelandet eller den berörda internationella organisationen har åtagit sig eller andra skyldigheter som uppstår på grund av juridiskt bindande konventioner eller instrument samt på grund av dess deltagande i multilaterala eller regionala system, i synnerhet i förhållande till skyddet av personuppgifter”.

eller hon föreslår att Förenade kungarikets framtida förordningar om adekvat skyddsnivå ska antas ([143]). När dessa förordningar har antagits av ministern läggs de fram inför parlamentet och omfattas av förfarandet för ”att rösta emot förordningen” enligt vilket båda kamrarna kan granska förordningen och kan anta ett förslag om att ogiltigförklara förordningen inom en 40-dagarsperiod ([144]).

(78) Enligt avsnitt 74B.1 i dataskyddslagen från 2018 ska bestämmelserna om adekvat skyddsnivå ses över med högst fyra års mellanrum och ministern ska fortlöpande övervaka utvecklingen i tredjeländer och internationella organisationer som skulle kunna påverka beslut om att utfärda föreskrifter om adekvat skyddsnivå eller att ändra eller upphäva sådana föreskrifter. Om ministern får kännedom om att ett visst land eller en organisation inte längre säkerställer en adekvat skyddsnivå för personuppgifter ska han eller hon, i den utsträckning det är nödvändigt, ändra eller upphäva föreskrifterna och inleda samråd med det berörda tredjelandet eller den berörda internationella organisationen för att avhjälpa bristen på adekvat skyddsnivå.

(79) I likhet med vad som föreskrivs i artikel 37 i direktiv (EU) 2016/680 skulle en överföring av personuppgifter inom ramen för den brottsbekämpande sektorn vara möjlig när lämpliga skyddsåtgärder har införts i avsaknad av en förordning om adekvat skyddsnivå. Sådana skyddsåtgärder säkerställs genom antingen a) ett rättsligt bindande instrument som innehåller lämpliga skyddsåtgärder för personuppgifter eller b) en bedömning utförd av den personuppgiftsansvariga som, efter att ha bedömt alla omständigheter kring överföringen, drar slutsatsen att det finns lämpliga skyddsåtgärder för att skydda uppgifterna ([145]). När överföringar grundar sig på lämpliga skyddsåtgärder föreskriver dataskyddslagen från 2018 dessutom att de behöriga myndigheterna, utöver ICO normala tillsynsroll, måste lämna specifik information om överföringarna till ICO ([146]).

(80) Om en överföring inte grundar sig på ett beslut om adekvat skyddsnivå eller lämpliga skyddsåtgärder kan den endast ske under vissa, specificerade omständigheter, så kallade särskilda omständigheter ([147]). Detta är fallet när överföringen är nödvändig a) för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan person, b) för att skydda den registrerades berättigade intressen, c) för att avvärja ett omedelbart och allvarligt hot mot den allmänna säkerheten i ett tredjeland, d) för att i enskilda fall för något av de brottsbekämpande ändamålen eller e) för att i enskilda fall för ett rättsligt ändamål (t.ex. i samband med rättsliga förfaranden eller för att erhålla juridisk rådgivning) ([148]). Det kan noteras att leden d) och e) inte är tillämpliga om den registrerades rättigheter och friheter väger tyngre än det allmänna intresset för överföringen ([149]). Dessa omständigheter motsvarar de särskilda situationer och villkor som räknas som ”undantag” enligt artikel 38 i direktiv (EU) 2016/680.

(81) Under dessa omständigheter ska datum, tidpunkt och motivering för överföringen, namnet på och all annan relevant information om mottagaren samt en beskrivning av de överförda personuppgifterna dokumenteras och på begäran lämnas till *Information Commissioner* ([150]).

(82) I avsnitt 78 i dataskyddslagen från 2018 regleras scenariot med ”efterföljande överföringar”, nämligen när personuppgifter som har överförts från Förenade kungariket till ett tredjeland senare överförs till ett annat tredjeland eller en internationell organisation. Enligt avsnitt 78.1 måste den överförande personuppgiftsansvariga i Förenade kungariket ställa som villkor för överföringen att uppgifterna inte ska överföras vidare till ett tredjeland utan den överförande personuppgiftsansvarigas tillstånd. I de fall ett sådant tillstånd krävs måste dessutom ett antal materiella villkor uppfyllas enligt avsnitt 78.3, och i likhet med vad som föreskrivs i artikel 35.1 e i direktiv (EU) 2016/680. En behörig myndighet som fattar beslut om huruvida överföringen ska tillåtas eller inte, måste se till att

([143]) Se samförståndsavtalet mellan ministern för *Department for Digital, Culture, Media and Sport* och ICO om ICO:s roll i samband med Förenade kungarikets nya bedömningar av adekvat skyddsnivå, finns på följande länk: https://www.gov.uk/government/publications/memorandum-of-understanding-mou-on-the-role-of-the-ico-in-relation-to-new-uk-adequacy-assessments.

([144]) Under denna 40-dagarsperiod kan båda kamrarna i parlamentet, om de så önskar, ha möjlighet att rösta emot förordningarna, om en sådan omröstning antas kommer förordningarna i slutändan att upphöra att ha någon ytterligare rättslig verkan.

([145]) Avsnitt 75 i dataskyddslagen från 2018.

([146]) Enligt avsnitt 75.3 i dataskyddslagen från 2018 om en överföring av uppgifter sker med stöd av lämpliga skyddsåtgärder gäller att a) överföringen ska dokumenteras, b) dokumentationen ska på begäran lämnas till Commissioner och c) dokumentationen ska särskilt innehålla i) datum och tidpunkt för överföringen, ii) namnet på och all annan relevant information om mottagaren, iii) motiveringen till överföringen och iv) en beskrivning av de personuppgifter som överförts.

([147]) *Guide to Law Enforcement Processing ”Are there any special circumstances?”* finns på följande länk: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/international-transfers/#ib3).

([148]) Avsnitt 76 i dataskyddslagen från 2018.

([149]) Avsnitt 76 i dataskyddslagen från 2018.

([150]) Avsnitt 76.3 i dataskyddslagen från 2018.

den ytterligare överföringen är nödvändig för ett brottsbekämpande ändamål och bör bland annat beakta a) hur allvarliga omständigheter som ledde till begäran om tillstånd, b) det ändamål för vilket personuppgifterna ursprungligen överfördes och c) de standarder för skydd av personuppgifter som gäller i det tredjeland eller den internationella organisation till vilken personuppgifterna skulle överföras.

(83) Dessutom gäller ytterligare skyddsåtgärder om de uppgifter som är föremål för vidare överföring från Förenade kungariket ursprungligen har överförts från Europeiska unionen.

(84) För det första föreskrivs i avsnitt 73.1 b i dataskyddslagen från 2018 – i likhet med vad som föreskrivs i artikel 35.1 c i direktiv (EU) 2016/680 – att om personuppgifterna ursprungligen överfördes eller på annat sätt gjordes tillgängliga för den personuppgiftsansvariga eller för en annan behörig myndighet av en medlemsstat, den medlemsstaten eller en person som är baserad i den medlemsstaten och som är en behörig myndighet enligt direktiv (EU) 2016/680, måste ha tillåtit överföringen i enlighet med medlemsstatens lagstiftning.

(85) I likhet med artikel 35.2 i direktiv (EU) 2016/680 krävs emellertid inte ett sådant tillstånd om a) överföringen är nödvändig för att avvärja ett omedelbart och allvarligt hot mot den allmänna säkerheten i en medlemsstat eller ett tredjeland eller mot en medlemsstats väsentliga intressen och b) tillståndet inte kan erhållas i tid. I detta fall ska den myndighet i medlemsstaten som skulle ha varit ansvarig för att besluta om tillstånd till överföringen underrättas utan dröjsmål ([151]).

(86) För det andra gäller samma tillvägagångssätt om uppgifter som ursprungligen överförts från Europeiska unionen till Förenade kungariket sedan överförs av Förenade kungariket till ett tredjeland, som därefter överför uppgifterna vidare till ett tredjeland. I sådana fall föreskriver avsnitt 78.4 att Förenade kungarikets behöriga myndighet inte kan ge tillstånd till den senare överföringen, enligt avsnitt 78.1, om inte ”den medlemsstat som först hade överfört uppgifterna i fråga, eller en person som är baserad i den medlemsstaten och som är en behörig myndighet enligt direktivet om uppgiftsskydd vid brottsbekämpning, har tillåtit överföringen i enlighet med medlemsstatens lagstiftning”. Dessa skyddsåtgärder är viktiga, eftersom de gör det möjligt för medlemsstaternas myndigheter att garantera skyddet genom hela ”överföringskedjan”, i enlighet med EU:s dataskyddslagstiftning.

(87) Denna nya ram för internationella överföringar började gälla i slutet av övergångsperioden ([152]). I punkterna 10–12 i tillägg 21 (införd genom DPPC-förordningarna) föreskrivs emellertid att vissa överföringar av personuppgifter från och med övergångsperiodens utgång behandlas som om de grundar sig på förordningar om adekvat skyddsnivå. Dessa överföringar omfattar överföringar till en medlemsstat, en Eftastat, ett tredjeland som är föremål för ett EU-beslut om adekvat skyddsnivå vid övergångsperiodens utgång samt territoriet Gibraltar. Följaktligen kan överföringarna till dessa länder fortsätta som före Förenade kungarikets utträde ur unionen. Efter övergångsperiodens utgång måste ministern under en fyraårsperiod, dvs. före utgången av december 2024, göra en översyn av dessa konstateranden om adekvat skyddsnivå. Enligt den förklaring som lämnats av Förenade kungarikets myndigheter innehåller övergångsbestämmelserna inte någon bestämmelse om tidsbegränsning, även om ministern måste göra en sådan översyn senast i slutet av december 2024, och de relevanta övergångsbestämmelserna kommer inte automatiskt att upphöra att gälla om en översyn inte är slutförd i slutet av december 2024.

2.4.9 *Ansvarsskyldighet*

(88) Enligt principen om ansvarsskyldighet är offentliga myndigheter som behandlar uppgifter skyldiga att vidta lämpliga tekniska och organisatoriska åtgärder för att effektivt uppfylla sina skyldigheter i fråga om dataskydd och kunna visa detta, särskilt för den behöriga tillsynsmyndigheten.

(89) Denna princip återspeglas i avsnitt 56 i dataskyddslagen från 2018, som inför en allmän redovisningsskyldighet för den personuppgiftsansvariga, dvs. en skyldighet att genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen av personuppgifter uppfyller kraven i del 3 i dataskyddslagen från 2018. De åtgärder som genomförs måste vid behov ses över och uppdateras och om de står i proportion till behandlingen inbegripa lämpliga dataskyddspolicyer.

([151]) Avsnitt 73.5 i dataskyddslagen från 2018.

([152]) Tillämpligheten för denna nya ram måste läsas mot bakgrund av artikel 782 i avtalet om handel och samarbete mellan Europeiska unionen och Europeiska atomenergigemenskapen, å ena sidan, och Förenade konungariket Storbritannien och Nordirland, å andra sidan (L 444/14, 31.12.2020) (*TCA mellan EU och Förenade kungariket*) som finns på följande länk: https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:22020A1231(01)&from=EN.

(90) I enlighet med kapitel IV i direktiv (EU) 2016/680 innehåller avsnitten 55–71 i dataskyddslagen från 2018 olika mekanismer för att säkerställa ansvarsskyldighet och göra det möjligt för personuppgiftsansvariga och personuppgiftsbiträden att visa efterlevnad. Personuppgiftsansvariga är särskilt skyldiga att genomföra inbyggt skydd av datauppgifter och skydd av datauppgifter som standard, dvs. att säkerställa att dataskyddsprinciperna genomförs på ett effektivt sätt och att de är skyldiga att föra register över alla kategorier av behandling av uppgifter som den personuppgiftsansvariga ansvarar för (inklusive information om den personuppgiftsansvarigas identitet, dataskyddsombudets kontaktuppgifter, ändamålen med behandlingen, kategorierna av mottagare av utlämnanden och en beskrivning av kategorierna av registrerade och personuppgifter) och på begäran hålla dessa register tillgängliga för *Information Commissioner*. Den personuppgiftsansvariga och personuppgiftsbiträdet måste också föra loggar över viss behandling och göra dem tillgängliga för *Information Commissioner* ([153]). De personuppgiftsansvariga är också särskilt skyldiga att samarbeta med *Information Commissioner* när han eller hon utför sina uppgifter.

(91) I dataskyddslagen från 2018 fastställs också ytterligare krav för behandling som sannolikt kommer att leda till en hög risk för enskildas rättigheter och friheter. Dessa inbegriper en skyldighet att genomföra konsekvensbedömningar avseende dataskydd och att samråda med *Information Commissioner* före behandlingen om en sådan bedömning visar att behandlingen skulle leda till en hög risk för enskildas rättigheter och friheter (i avsaknad av åtgärder för att minska risken).

(92) De personuppgiftsansvariga måste dessutom utse ett dataskyddsombud, såvida inte den personuppgiftsansvariga är en domstol eller annan rättslig myndighet som agerar i egenskap av domstol ([154]). Den personuppgiftsansvariga ska se till att dataskyddsombudet är involverat i alla frågor som rör skydd av personuppgifter, har nödvändiga resurser och tillgång till personuppgifter, behandlar personuppgifter och kan utföra sina uppgifter på ett oberoende sätt. Dataskyddsombudets uppgifter anges i avsnitt 71 i dataskyddslagen från 2018 och är bland annat att tillhandahålla information och rådgivning, övervaka efterlevnaden samt samarbeta med och fungera som kontaktpunkt för *Information Commissioner*. När dataskyddsombudet utför sina uppgifter ska han eller hon ta hänsyn till de risker som är förenade med behandlingen med beaktande av behandlingens art, omfattning, sammanhang och ändamål.

2.5 **Tillsyn och efterlevnad**

2.5.1 *Oberoende tillsyn*

(93) För att säkerställa att en adekvat skyddsnivå för personuppgifter garanteras även i praktiken måste det finnas en oberoende tillsynsmyndighet med befogenhet att övervaka och verkställa efterlevnaden av dataskyddsbestämmelserna. Denna myndighet ska agera fullständigt oberoende och opartiskt vid utförandet av sina uppgifter och utövandet av sina befogenheter.

(94) I Förenade kungariket övervakas och verkställs efterlevnaden av den brittiska dataskyddsförordningen och dataskyddslagen från 2018 av *Information Commissioner* ([155]). *Information Commissioner* övervakar också de behöriga myndigheternas behandling av personuppgifter som omfattas av del 3 i dataskyddslagen från 2018 ([156]). *Information Commissioner* är en juridisk person, en separat juridisk person som består av en enda person. *Information Commissioner* bistås i sitt arbete av ett kontor (ICO). Den 31 mars 2020 hade ICO 768 fast anställda ([157]). Den uppdragsgivande avdelningen för *Information Commissioner* är Department for Digital, Culture, Media and Sport ([158]).

([153]) Avsnitt 62 i dataskyddslagen från 2018.
([154]) Avsnitt 69 i dataskyddslagen från 2018.
([155]) Artikel 36.2 b i direktiv (EU) 2016/680.
([156]) Avsnitt 116 i dataskyddslagen från 2018.
([157]) *Information Commissioner's Annual Report and Financial Statements 2019–2020*, som finns på följande länk: https://ico.org.uk/media/about-the-ico/documents/2618021/annual-report-2019-20-v83-certified.pdf
([158]) Ett förvaltningsavtal reglerar förhållandet mellan dem. De viktigaste uppgifterna för departementet för digitala frågor, kultur, media och idrott, i egenskap av uppdragsgivande avdelning, omfattar följande: Säkerställa att ICO får tillräcklig finansiering och tillräckliga resurser. Företräda ICO:s intressen inför parlamentet och andra regeringsdepartement. Se till att det finns en stabil nationell ram för dataskydd. Ge vägledning och stöd till ICO i företagsfrågor som fastighets-, hyres- och upphandlingsfrågor (förvaltningsavtalet 2018–2021 finns på följande länk: https://ico.org.uk/media/about-the-ico/documents/2259800/management-agreement-2018-2021.pdf).

(95) Oberoendet för *Commissioner* fastställs uttryckligen i artikel 52 i den brittiska dataskyddsförordningen som återspeglar kraven i artikel 52.1–52.3 i Europaparlamentets och rådets förordning (EU) 2016/679 ([159]). *Commissioner* måste agera fullständigt oberoende vid utförandet av sina uppgifter och utöva sina befogenheter i enlighet med den brittiska dataskyddsförordningen, vara fri från yttre påverkan, direkt eller indirekt, i förhållande till dessa uppgifter och befogenheter och varken begära eller ta emot instruktioner från någon. *Commissioner* ska också avhålla sig från varje handling som är oförenlig med hans eller hennes uppdrag och får inte utöva någon avlönad eller oavlönad yrkesverksamhet under tiden som han eller hon innehar sitt ämbete.

(96) Villkoren för utnämning och avsättning av *Information Commissioner* anges i tillägg 12 till dataskyddslagen från 2018. *Information Commissioner* utses av drottningen på rekommendation av regeringen i enlighet med ett rättvist och öppet uttagningsförfarande. Den sökande måste ha lämpliga kvalifikationer, färdigheter och kompetenser. I enlighet med förvaltningskodexen om offentliga utnämningar ([160]) upprättas en förteckning över kandidater som kan utnämnas av en rådgivande utvärderingspanel. Innan ministern vid Department for Digital, Culture, Media and Sport slutför sitt beslut måste det berörda särskilda utskottet i parlamentet genomföra en kontroll före utnämningen. Utskottets ståndpunkt offentliggörs ([161]).

(97) *Information Commissioner* har en mandatperiod på upp till sju år. Information Commissioner kan avsättas av drottningen efter ett anförande i båda kamrarna i parlamentet ([162]). En begäran om entledigande av *Information Commissioner* kan inte lämnas in till någon av parlamentets kammare om inte en minister har lagt fram en rapport till kammaren där det anges att ministern är övertygad om att *Information Commissioner* gjort sig skyldig till allvarlig försummelse och/eller att denna inte längre uppfyller de villkor som krävs för att kunna fullgöra sina uppgifter ([163]).

(98) Finansieringen av *Information Commissioner* kommer från följande tre källor: i) Avgifter för dataskydd som betalas av personuppgiftsansvariga och som fastställs i ministerns förordningar ([164]) och uppgår till 85–90 % av myndighetens årliga budget ([165]). ii) Bidrag i form av stöd som regeringen kan betala ut till *Information Commissioner* och som huvudsakligen används för att finansiera driftskostnaderna för *Information Commissioner* när det gäller uppgifter som inte rör dataskydd ([166]). iii) Avgifter som tas ut för tjänster ([167]). För närvarande tas inga sådana avgifter ut.

(99) De allmänna uppgifterna för *Information Commissioner* när det gäller behandling av personuppgifter som omfattas av del 3 i dataskyddslagen från 2018 fastställs i tillägg 13 till dataskyddslagen från 2018. Uppgifterna omfattar övervakning och genomförande av del 3 i dataskyddslagen från 2018, främjande av allmänhetens medvetenhet, rådgivning till parlamentet, regeringen och andra institutioner om lagstiftningsåtgärder och administrativa åtgärder, främjande av personuppgiftsansvarigas och personuppgiftsbiträdens medvetenhet om deras skyldigheter, tillhandahållande av information till registrerade om utövandet av den registrerades rättigheter samt genomförande av

([159]) Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1).

([160]) Styrningskoden för offentliga utnämningar, finns på följande länk: https://www.gov.uk/government/publications/governance-code-for-public-appointments.

([161]) Andra rapporten från sammanträdesperioden 2015–2016 från utskottet för kultur, medier och idrott i underhuset finns på följande länk: https://publications.parliament.uk/pa/cm201516/cmselect/cmcumeds/990/990.pdf

([162]) Ett ”anförande” är ett förslag som lagts fram för parlamentet och som syftar till att göra monarken medveten om parlamentets yttranden i en viss fråga.

([163]) Punkt 3 i bilaga 12 till dataskyddslagen från 2018.

([164]) Avsnitt 137 i dataskyddslagen från 2018.

([165]) Avsnitten 137 och 138 i dataskyddslagen från 2018 innehåller ett antal skyddsåtgärder för att säkerställa att avgifterna fastställs på en lämplig nivå. I avsnitt 137.4 i dataskyddslagen från 2018 anges särskilt de omständigheter som ministern ska beakta när han eller hon fastställer det belopp som olika organisationer ska betala. Avsnitt 138.1 och avsnitt 182 i dataskyddslagen från 2018 innehåller också en rättslig skyldighet för ministern att samråda med Information Commissioner och andra företrädare för personer som kan komma att beröras av förordningarna innan de framförs så att deras synpunkter kan beaktas. Enligt avsnitt 138.2 i dataskyddslagen från 2018 är Information Commissioner dessutom skyldig att se över avgiftsförordningarnas funktion och kan lämna förslag till ministern om ändringar av förordningarna. Slutligen, utom i de fall då bestämmelser endast utarbetas för att ta hänsyn till en ökning av konsumentprisindex (då de kommer att omfattas av ett negativt resolutionsförfarande), omfattas föreskrifterna av ett positivt resolutionsförfarande och får inte utfärdas förrän de har godkänts genom ett beslut av varje kammare.

([166]) I förvaltningsavtalet klargjordes att ”ministern får göra utbetalningar till Information Commissioner med medel som tillhandahålls av parlamentet enligt punkt 9 i tillägg 12 till dataskyddslagen från 2018. Efter samråd med Information Commissioner ska DCMS betala lämpliga belopp (bidraget i form av stöd) för ICO:s administrativa kostnader och utövandet av de uppgifter som Information Commissioner har i samband med ett antal specifika funktioner, däribland informationsfrihet” (förvaltningsavtal 2018–2021, punkt 1.12, se fotnot 158).

([167]) Avsnitt 134 i dataskyddslagen från 2018.

utredningar. För att upprätthålla rättsväsendets oberoende är *Information Commissioner* inte behörig att utföra sina uppgifter i samband med behandling av personuppgifter som utförs av en enskild person som handlar i egenskap av en dömande myndighet eller av en domstol som agerar inom ramen för sin dömande verksamhet. Tillsynen över rättsväsendet säkerställs dock av specialiserade organ som diskuteras nedan.

2.5.1.1 Verkställighet, inklusive påföljder

(100) *Commissioner* har allmänna undersökande, korrigerande, tillståndsgivande och rådgivande befogenheter när det gäller behandling av personuppgifter som omfattas av del 3 i dataskyddslagen från 2018. *Commissioner* har befogenhet att underrätta den personuppgiftsansvariga eller personuppgiftsbiträdet om en påstådd överträdelse av del 3, utfärda varningar till en registeransvarig eller ett personuppgiftsbiträde om att planerad behandling sannolikt kommer att strida mot bestämmelserna i del 3 och utfärda reprimander till en personuppgiftsansvarig eller ett personuppgiftsbiträde om behandlingen har brutit mot bestämmelserna i del 3. Dessutom får *Commissioner* på eget initiativ eller på begäran avge yttranden till Förenade kungarikets parlament, regeringen eller andra institutioner och organ samt till allmänheten i alla frågor som rör skyddet av personuppgifter ([168]).

(101) Dessutom har *Commissioner* befogenhet att

— beordra den personuppgiftsansvariga och personuppgiftsbiträdet (och under vissa omständigheter varje annan person) att lämna nödvändig information genom ett informationsmeddelande (*informationsföreläggande*) ([169]),

— genomföra utredningar och revisioner genom att lämna ett bedömningsmeddelande, vilket kan kräva att den personuppgiftsansvariga eller personuppgiftsbiträdet ger *Commissioner* tillträde till särskilda lokaler, inspekterar eller undersöker handlingar eller utrustning, intervjuar personer som behandlar personuppgifter på den personuppgiftsansvarigas vägnar (*bedömningsföreläggande*) ([170]),

— på annat sätt få tillgång till personuppgiftsansvarigas och personuppgiftsbiträdens handlingar och tillträde till deras lokaler i enlighet med avsnitt 154 i dataskyddslagen från 2018 (*befogenheter för tillträde och inspektion*),

— utföra korrigerande befogenheter, bland annat genom varningar och reprimander eller utfärda förelägganden genom ett verkställighetsmeddelande som kräver att personuppgiftsansvariga/personuppgiftsbiträden vidtar eller avstår från att vidta specificerade åtgärder (*verkställighetsföreläggande*) ([171]) och

— utfärda administrativa sanktionsavgifter i form av ett bötesföreläggande (*påföljdsföreläggande*) ([172]).

(102) I ICO:s policy för lagstiftningsåtgärder anges under vilka omständigheter *Commissioner* kommer att utfärda ett meddelande om informations-, bedömnings-, verkställighets- respektive påföljdsföreläggande ([173]). Ett verkställighetsmeddelande kan ställa krav som *Commissioner* anser vara lämpliga för att avhjälpa underlåtenheten. Ett föreläggande om vite innebär att personen ska betala ett belopp som anges i meddelandet till *Information Commissioner*. Ett påföljdsföreläggande kan lämnas när vissa bestämmelser i dataskyddslagen från 2018 ([174]) inte har följts eller kan lämnas till en personuppgiftsansvarig eller ett personuppgiftsbiträde som inte har följt ett informationsföreläggande, ett bedömningsföreläggande eller ett verkställighetsföreläggande.

(103) När *Information Commissioner* avgör om en personuppgiftsansvarig eller ett personuppgiftsbiträde ska få ett påföljdsföreläggande och fastställa påföljdsbeloppet ska han eller hon ta hänsyn till de frågor som anges i avsnitt 155.3 i dataskyddslagen från 2018, inbegripet felets art och allvar, felets avsiktliga eller försumliga karaktär, alla åtgärder som vidtas av den personuppgiftsansvariga eller personuppgiftsbiträdet för att minska den skada som de registrerade lidit, den personuppgiftsansvarigas eller personuppgiftsbiträdets grad av ansvar (med beaktande av den

([168]) Punkt 2 i tillägg 13 till dataskyddslagen från 2018.
([169]) Avsnitt 142 i dataskyddslagen från 2018 (med förbehåll för begränsningarna i avsnitt 143 dataskyddslagen från 2018).
([170]) Avsnitt 146 i dataskyddslagen från 2018 (med förbehåll för begränsningarna i avsnitt 147 dataskyddslagen från 2018).
([171]) Avsnitten 149–151 i dataskyddslagen från 2018 (med förbehåll för begränsningarna i avsnitt 152 dataskyddslagen från 2018).
([172]) Avsnitt 155 i dataskyddslagen från 2018 (med förbehåll för begränsningarna i avsnitt 156 i dataskyddslagen från 2018).
([173]) Policyn för lagstiftningsåtgärder (Regulatory Action Policy), finns på följande länk: https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf.
([174]) ICO får särskilt utfärda ett meddelande om påföljd för bristande efterlevnad enligt avsnitt 149.2, 3, 4 eller 5 i dataskyddslagen från 2018.

personuppgiftsansvarigas eller personuppgiftsbiträdets tekniska och organisatoriska åtgärder), eventuella tidigare brister som den personuppgiftsansvariga eller personuppgiftsbiträdet har gjort sig skyldiga till, de kategorier av personuppgifter som berörs av underlåtenheten och huruvida sanktionen skulle vara effektiv, proportionell och avskräckande.

(104) Det högsta bötesbelopp som kan utdömas genom ett påföljdsföreläggande är a) 17 500 000 GBP för underlåtenhet att iaktta dataskyddsprinciperna (avsnitten 35, 36, 37, 38.1, 39.1och 40 i dataskyddslagen från 2018) transparenskrav och individuella rättigheter (avsnitten 44, 45, 46, 47, 48, 49, 52 och 53 i dataskyddslagen från 2018) och principer för internationella överföringar av personuppgifter (avsnitten 73, 75, 76, 77 eller 78 i dataskyddslagen från 2018) och b) 8 700 000 GBP i annat fall ([175]). När det gäller underlåtenhet att följa ett informationspåföljdsföreläggande, ett bedömningspåföljdsföreläggande eller ett verkställighetspåföljdsföreläggande är det högsta bötesbelopp som kan utdömas genom ett bötesföreläggande 17 500 000 GBP.

(105) Enligt sina senaste årsrapporter (2018–2019 ([176]), 2019–2020 ([177])) har *Information Commissioner* genomfört ett antal utredningar om kriminalvårdande myndigheters behandling av personuppgifter. Till exempel genomförde *Commissioner* en utredning och offentliggjorde ett yttrande i oktober 2019 om brottsbekämpande myndigheters användning av ansiktsigenkänningsteknik på offentliga platser. Utredningen inriktades särskilt på användningen av kapacitet för ansiktsigenkänning inom polisen i South Wales Police och Metropolitan Police Service (MPS). Dessutom undersökte *Commissioner* MPS "Gangs matrix" ([178]) och fann en rad allvarliga överträdelser av dataskyddslagstiftningen som sannolikt skulle undergräva allmänhetens förtroende för matrisen och användningen av uppgifterna.

(106) I november 2018 utfärdade *Information Commissioner* ett verkställighetspåföljdsföreläggande och därefter vidtog Metropolitan Police Service de åtgärder som krävdes för att öka säkerheten och ansvarsskyldigheten och se till att uppgifterna användes på ett proportionerligt sätt.

(107) Ett annat exempel på en nyligen genomförd verkställighetsåtgärd är de böter på 325 000 GBP som *Commissioner* utfärdade mot åklagarmyndigheten i maj 2018 för att ha förlorat okrypterade dvd-skivor som innehöll inspelningar av polisförhör. Dessutom genomförde *Information Commissioner* utredningar av bredare frågor, till exempel under första halvåret 2020 om användningen av mobiltelefonavlyssning för polisändamål och polisens behandling av offrens uppgifter.

(108) Utöver de verkställande befogenheterna för *Information Commissioner* utgör vissa överträdelser av dataskyddslagstiftningen brott och kan därför bli föremål för straffrättsliga påföljder (avsnitt 196 i dataskyddslagen från 2018). Detta gäller till exempel för inhämtande eller utlämnande av personuppgifter utan den personuppgiftsansvarigas samtycke och för utlämnande av personuppgifter till en annan person utan den personuppgiftsansvarigas samtycke ([179]), återidentifierande information som utgörs av avidentifierade personuppgifter utan samtycke från den personuppgiftsansvariga som ansvarar för avidentifieringen av personuppgifterna ([180]), avsiktligen hindra *Commissioner* från att utöva sina befogenheter när det gäller kontroll av personuppgifter i enlighet med internationella skyldigheter ([181]), lämna oriktiga uppgifter som svar på ett informationspåföljdsföreläggande eller förstöra information i samband med informations- och bedömningspåföljdsförelägganden ([182]).

(109) *Information Commissioner* har också en skyldighet enligt avsnitt 139 i dataskyddslagen från 2018 att för varje kammare lägga fram en allmän rapport om utövandet av sina uppgifter enligt lagen ([183]).

([175]) Avsnitt 157 i dataskyddslagen från 2018.

([176]) *Information Commissioner's Annual Report and Financial Statements 2018–2019*, som finns på följande länk: https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf

([177]) Information Commissioners årsredovisning 2019–2020 (se fotnot 157).

([178]) En databas med uppgifter om påstådda gruppmedlemmar och offer för gängrelaterade brott.

([179]) Avsnitt 170 i dataskyddslagen från 2018.

([180]) Avsnitt 171 i dataskyddslagen från 2018.

([181]) Avsnitt 119 i dataskyddslagen från 2018.

([182]) Avsnitt 144 och 148 i dataskyddslagen från 2018.

([183]) Enligt förvaltningsavtalet ska årsrapporten i) täcka alla företag, dotterbolag eller samriskföretag som står under kontroll av ICO, ii) följa finansministeriets handbok för finansiell rapportering (FReM), iii) innehålla en verksamhetsberättelse med en beskrivning av hur Accounting Officer har förvaltat och kontrollerat de resurser som används i organisationen under året, som visar hur väl organisationen hanterar risker när det gäller att uppnå sina syften och mål och iv) ge en översikt över de viktigaste verksamheterna och resultaten under det föregående budgetåret och sammanfatta preliminära planer (Management Agreement 2018–2021, punkt 3.26, se fotnot 158).

2.5.2 *Tillsyn över rättsväsendet*

(110) Tillsynen över domstolarnas och rättsväsendets behandling av personuppgifter är dubbel. Om en innehavare av ett domarämbete eller en domstol inte agerar inom ramen för sin dömande verksamhet ska tillsynen ombesörjas av *Information Commissioner*. Om den personuppgiftsansvariga agerar inom ramen för sin dömande verksamhet kan ICO inte utöva sina tillsynsfunktioner ([184]) utan tillsynen utförs av särskilda organ. Detta återspeglar tillvägagångssättet i artikel 32 i direktiv (EU) 2016/680.

(111) I synnerhet i det andra scenariot, för domstolarna i England och Wales samt förstainstansdomstolen och Upper Tribunal i England och Wales, tillhandahålls sådan tillsyn av *Judicial Data Protection Panel* ([185]). Lord Chief Justice och Chief President of Tribunals har dessutom utfärdat ett meddelande om skydd av personuppgifter ([186]) som beskriver hur domstolarna i England och Wales behandlar personuppgifter för en rättslig funktion. Ett liknande meddelande har utfärdats av de nordirländska ([187]) och skotska domstolarna ([188]).

(112) I Nordirland har dessutom Lord Chief Justice of Northern Ireland utsett en domare vid High Court som datatillsynsdomare (*Data Supervisory Judge*, DSJ) ([189]). De har också gett vägledning till det nordirländska domstolsväsendet om vad som ska göras i händelse av förlust eller potentiell förlust av uppgifter och förfarandet för att hantera eventuella problem som uppstår till följd av detta ([190]).

(113) I Skottland har Lord President utsett en datatillsynsdomare som ska utreda eventuella klagomål med hänvisning till dataskydd. Detta anges i de regler för klagomål till domstol som motsvarar dem som gäller för England och Wales ([191]).

(114) I högsta domstolen utses slutligen en av högsta domstolens domare för att övervaka dataskyddet.

([184]) Avsnitt 117 i dataskyddslagen från 2018.

([185]) Panelen ansvarar för att ge domstolsväsendet vägledning och utbildning. Den behandlar också klagomål från registrerade med avseende på behandling av personuppgifter som utförs av domstolar och enskilda personer som handlar i egenskap av en dömande myndighet. Panelen har för avsikt att tillhandahålla de medel som kan användas för att lösa eventuella klagomål. Om en klagande var missnöjd med panelens beslut och lade fram ytterligare bevisning skulle panelen kunna ompröva sitt beslut. Även om panelen själv inte utdömer ekonomiska sanktioner kan den, om den anser att det föreligger en tillräckligt klar överträdelse av dataskyddslagen från 2018, hänskjuta den till JCIO (*Judicial Conduct Investigation Office*), som kommer att utreda klagomålet. Om klagomålet godtas ankommer det på Lord Chancellor och Lord Chief Justice (eller en högre domare som delegerats att agera på hans eller hennes vägnar) att besluta om vilka åtgärder som ska vidtas mot befattningshavaren. Detta kan, beroende på svårighetsgrad, omfatta formell rådgivning, formell varning och reprimand och, i slutändan, entledigande. Om en person är missnöjd med det sätt på vilket klagomålet har utretts av JCIO kan han eller hon lämna in ett klagomål till *Judicial Appointments and Conduct Ombudsman* (se https://www.gov.uk/government/organisations/judicial-appointments-and-conduct-ombudsman). Ombudsmannen har befogenhet att be JCIO att utreda ett klagomål på nytt och kan föreslå att klaganden ska få ersättning om han eller hon anser sig ha lidit skada till följd av administrativa missförhållanden.

([186]) Meddelandet om skydd av personuppgifter från Lord Chief Justice and Senior President of Tribunals, finns på följande länk: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice

([187]) Meddelande om skydd av personuppgifter från Lord Chief Justice of Northern Ireland, finns på följande länk: https://judiciaryni.uk/data-privacy

([188]) Meddelandet om skydd av personuppgifter för skotska domstolar och tribunaler finns på följande länk: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice

([189]) Datatillsynsdomaren ger vägledning till rättsväsendet och utreder överträdelser och/eller klagomål som rör behandling av personuppgifter som utförs av domstolar eller enskilda personer som handlar i egenskap av en dömande myndighet.

([190]) Om klagomålet eller brottet bedöms vara allvarligt hänskjuts det till *Judicial Complaints Officer* för vidare utredning i enlighet med *Lord Chief Justice in Northern Ireland's Code of Practice on Complaints*. Ett sådant klagomål skulle kunna omfatta inga ytterligare åtgärder, råd, utbildning eller mentorskap, informell varning, formell varning, slutlig varning, begränsning av praxis eller hänskjutande till en lagstadgad domstol. *Code of Practice on Complaints* som utfärdats av Lord Chief Justice i Nordirland finns på följande länk: https://judiciaryni.uk/sites/judiciary/files/media-files/14G.%20CODE%20OF%20PRACTICE%20Judicial%20~%2028%20Feb%2013%20%28Final%29%20updated%20with%20new%20comp..__1.pdf.

([191]) Varje klagomål utreds av en datatillsynsdomare och hänskjuts till Lord President som har befogenhet att utfärda råd, en formell varning eller en reprimand om han anser det nödvändigt (likvärdiga regler finns för domstolsledamöter och de finns på följande länk: https://www.judiciary.scot/docs/librariesprovider3/judiciarydocuments/complaints/complaintsaboutthejudiciaryscotlandrules2017_1d392ab6e14f6425aa0c7f48d062f5cc5.pdf?sfvrsn=5d3eb9a1_2).

2.5.3 *Prövningsmöjligheter*

(115) För att säkerställa adekvat skydd, och i synnerhet tillämpningen av individuella rättigheter, bör den registrerade erbjudas möjligheten till faktisk administrativ och rättslig prövning, inbegripet ersättning för skador.

(116) För det första har den registrerade rätt att lämna in ett klagomål till *Information Commissioner* om den registrerade anser att det i samband med personuppgifter som rör honom eller henne föreligger en överträdelse av del 3 i dataskyddslagen från 2018 ([192]). Enligt skälen (100) och (109) har *Information Commissioner* befogenhet att bedöma den personuppgiftsansvarigas och personuppgiftsbiträdets efterlevnad av dataskyddslagen från 2018, kräva att de vidtar eller avstår från att vidta nödvändiga åtgärder vid bristande efterlevnad och utdöma sanktionsavgifter.

(117) För det andra föreskriver dataskyddslagen från 2018 en rätt till rättsmedel mot *Information Commissioner*. Om *Commissioner* underlåter att ”gå vidare” ([193]) med ett klagomål från den registrerade har klaganden tillgång till rättsmedel eftersom de kan vända sig till en förstainstansdomstol ([194]) för att beordra *Commissioner* att vidta lämpliga åtgärder för att besvara klagomålet eller informera den klagande om hur ärendet fortskrider ([195]). Dessutom kan varje person som får något av ovanstående påföljdsföreläggande (informations-, bedömnings-, verkställighets- eller påföljdspåföljdsföreläggande) från *Commissioner* överklaga till en förstainstansdomstol. Om tribunalen anser att beslutet från *Commissioner* inte är förenligt med lagen eller att *Information Commissioner* borde ha utövat sitt utrymme för skönsmässig bedömning på ett annat sätt, ska tribunalen bifalla överklagandet eller ersätta ett annat föreläggande eller beslut som *Information Commissioner* skulle ha kunnat lämna eller fatta ([196]).

(118) För det tredje kan enskilda få rättslig prövning mot personuppgiftsansvariga och personuppgiftsbiträden direkt vid domstol enligt avsnitt 167 i dataskyddslagen från 2018. Om en domstol på begäran av en registrerad är övertygad om att det har skett en överträdelse av den registrerades rättigheter enligt dataskyddslagstiftningen får domstolen förelägga den personuppgiftsansvariga att vidta de åtgärder som anges i beslutet eller att avstå från att vidta de åtgärder som anges i beslutet. Enligt avsnitt 169 i dataskyddslagen från 2018 har dessutom varje person som lider skada till följd av en överträdelse av ett krav i dataskyddslagstiftningen (inklusive del 3 i dataskyddslagen från 2018), med undantag för Förenade kungarikets dataskyddsmyndighet, rätt till ersättning för denna skada från den personuppgiftsansvariga eller personuppgiftsbiträdet, förutom om den personuppgiftsansvariga eller personuppgiftsbiträdet bevisar att den personuppgiftsansvariga eller personuppgiftsbiträdet inte på något sätt är ansvarig för den händelse som orsakade skadan. Med skada avses både ekonomisk förlust och skada som inte medför ekonomiska förluster, till exempel nödläge.

(119) För det fjärde, i den mån som en person anser att hans eller hennes rättigheter, inbegripet rätten till integritet och dataskydd, har kränkts av offentliga myndigheter kan de få sin sak prövad av domstolar i Förenade kungariket i enlighet med *Human Rights Act 1998*. De personuppgiftsansvariga enligt del 3 i dataskyddslagen från 2018, dvs. de behöriga myndigheterna, är alltid offentliga myndigheter i den mening som avses i *Human Rights Act 1998*. En enskild som hävdar att en offentlig myndighet har agerat (eller avser att agera) på ett sätt som är oförenligt med en rättighet enligt konventionen, och följaktligen är olagligt enligt avsnitt 6.1 i *Human Rights Act 1998*, kan väcka talan mot myndigheten vid behörig domstol eller åberopa de berörda rättigheterna i ett rättsligt förfarande när han eller hon är (eller skulle bli) offer för den olagliga handlingen ([197]).

([192]) Avsnitt 165 i dataskyddslagen från 2018.

([193]) I avsnitt 166 i dataskyddslagen från 2018 hänvisas särskilt till situationerna att a) Commissioner underlåter att vidta lämpliga åtgärder för att besvara klagomålet, b) kommissionären underlåter att informera den klagande om hur ärendet fortskrider eller om resultatet av klagomålet före utgången av den period på tre månader som började när kommissionären mottog klagomålet eller c) om kommissionärens behandling av klagomålet inte avslutas under den perioden inte ger klaganden sådan information under en senare tremånadersperiod.

([194]) Förstainstansdomstolen är behörig att handlägga överklaganden av beslut som fattats av statliga tillsynsorgan. När det gäller beslut av Information Commissioner är den behöriga avdelningen ”General Regulatory Chamber” som är behörig i hela Förenade kungariket.

([195]) Avsnitt 166 i dataskyddslagen från 2018.

([196]) Avsnitt 161 och 162 i dataskyddslagen från 2018.

([197]) Se målet Brown/Commissioner of the Met 2016 där domstolen gav käranden upprättelse i samband med dataskydd i samband med en talan mot polisen. Domstolen biföll den kärandes påståenden om åsidosättande av skyldigheterna enligt dataskyddslagen från 1998, åsidosättande av HRA 1998 (och den närstående rättigheten i artikel 8 i Europakonventionen) och skadeståndsgrundande missbruk av privat information (svaranden medgav slutligen att de stred mot dataskyddslagen och den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna, så domen fokuserade på vilket rättsmedel som var lämpligt). Till följd av dessa åsidosättanden tilldömde domstolen käranden ekonomisk ersättning.

(120) Om domstolen finner att en åtgärd som vidtas av en offentlig myndighet är rättsstridig kan den bevilja en sådan befrielse eller ett sådant rättsmedel eller fatta ett sådant beslut inom ramen för sina befogenheter som den anser vara skäligt och lämpligt ([198]). Domstolen kan också förklara att en primärrättslig bestämmelse är oförenlig med en rättighet som garanteras i Europakonventionen.

(121) Slutligen kan en enskild, efter att ha uttömt nationella rättsmedel, vända sig till Europeiska domstolen för de mänskliga rättigheterna för kränkningar av de rättigheter som garanteras enligt Europakonventionen.

2.6 **Fortsatt delning**

(122) Enligt Förenade kungarikets lag får en brottsbekämpande myndighet dela uppgifter med andra myndigheter i Förenade kungariket för andra ändamål än de för vilka de ursprungligen samlades in (så kallad vidaredelning) på vissa villkor.

(123) I likhet med vad som föreskrivs i artikel 4.2 i direktiv (EU) 2016/680 tillåter avsnitt 36.3 i dataskyddslagen från 2018 att personuppgifter som samlats in av en behörig myndighet för brottsbekämpande ändamål får behandlas ytterligare (antingen av den ursprungliga personuppgiftsansvariga eller av en annan registeransvarig) för andra brottsbekämpande ändamål, förutsatt att den personuppgiftsansvariga enligt lag är bemyndigad att behandla uppgifter för det andra ändamålet och att behandlingen är nödvändig och proportionell ([199]). I detta fall gäller alla skyddsåtgärder som föreskrivs i del 3 i dataskyddslagen från 2018 och som analyserats ovan för den behandling som utförs av den mottagande myndigheten.

(124) I Förenade kungarikets rättsordning tillåter olika lagar uttryckligen vidaredelning. I synnerhet i) 2017 års lag om den digitala ekonomin tillåter delning mellan offentliga myndigheter för flera ändamål, till exempel vid bedrägeri mot den offentliga sektorn som skulle innebära förlust eller risk för förlust för en offentlig myndighet ([200]) eller vid en skuld till en offentlig myndighet eller till staten ([201]), ii) *Crime and Courts Act 2013* tillåter utbyte av information med National Crime Agency (NCA) ([202]) för bekämpning, utredning och lagföring av grov och organiserad brottslighet, iii) enligt *Serious Crime Act 2007* får offentliga myndigheter lämna ut information till bedrägeribekämpningsorganisationer för att förebygga bedrägerier ([203]).

(125) I dessa lagar föreskrivs uttryckligen att informationsutbytet bör ske i enlighet med bestämmelserna i dataskyddslagen från 2018. Dessutom har polisakademin utfärdat en auktoriserad yrkespraxis för informationsutbyte ([204]) för att hjälpa polisen att uppfylla sina dataskyddsskyldigheter enligt den brittiska dataskyddsförordningen, dataskyddslagen och *Human Rights Act 1998*. Naturligtvis kan det bli föremål för rättslig prövning av huruvida utbytet överensstämmer med den tillämpliga rättsliga ramen för dataskydd ([205]).

(126) I likhet med vad som anges i artikel 9 i direktiv (EU) 2016/680 föreskriver dataskyddslagen från 2018 dessutom att personuppgifter som samlas in för brottsbekämpningsändamål får behandlas för ett ändamål som inte är brottsbekämpningssyfte när behandlingen är tillåten enligt lag ([206]). Denna typ av delning omfattar två scenarier 1) när en brottsbekämpande myndighet delar uppgifter med en annan icke-straffrättslig brottsbekämpande myndighet än en underrättelsetjänst (t.ex. en finans- eller skattemyndighet, en konkurrensmyndighet, en ungdomsmyndighet),

([198]) Avsnitt 8.1 i *Human Rights Act 1998*.
([199]) Avsnitt 36.3 i dataskyddslagen från 2018.
([200]) Avsnitt 56 i *Digital Economy Act 2017* finns på följande länk: https://www.legislation.gov.uk/ukpga/2017/30/contents
([201]) Avsnitt 48 i *Digital Economy Act 2017*.
([202]) Avsnitt 7 i *Crime and Courts Act 2013*, finns på följande länk: https://www.legislation.gov.uk/ukpga/2013/22/contents
([203]) Avsnitt 68 i *Serious Crime Act 2007* finns på följande länk: https://www.legislation.gov.uk/ukpga/2007/27/contents
([204]) Den godkända yrkesmässiga praxisen för informationsutbyte finns på följande länk: https://www.app.college.police.uk/app-content/information-management/sharing-police-information
([205]) Se till exempel målet M/Chief Constable of Sussex Police [2019] EWHC 975 (Admin) där High Court ombads att överväga utbyte av uppgifter mellan polisen och Business Crime Reduction Partnership (BCRP), en organisation som har befogenhet att förvalta systemet för uteslutning och som förbjuder personer att komma in i medlemmarnas affärslokaler. Domstolen granskade datadelningen som ägde rum på grundval av ett avtal som syftade till att skydda allmänheten och förebygga brott och kom slutligen fram till att de flesta aspekterna av datadelning var lagliga utom när det gäller viss känslig information som delas mellan polisen och de grundläggande rättigheterna. Ett annat exempel är målet Cooper/NCA [2019] EWCA Civ 16, där appellationsdomstolen bekräftade datadelningen mellan polisen och Serious Organised Crime Agency (SOCA), en brottsbekämpande myndighet som för närvarande ingår i NCA (nationella konkurrensmyndigheten).
([206]) Avsnitt 36.4 i dataskyddslagen från 2018.

2) när en brottsbekämpande myndighet delar uppgifter med en underrättelsetjänst. I det första scenariot kommer behandlingen av personuppgifter att omfattas av den brittiska dataskyddsförordningen och av del 2 i dataskyddslagen från 2018. Enligt det beslut som antagits enligt förordning (EU) 2016/679 ger de skyddsåtgärder som föreskrivs i Förenade kungarikets allmänna dataskyddsförordning och del 2 i dataskyddslagen från 2018 en skyddsnivå som i allt väsentligt är likvärdig med den som ges inom unionen ([207]).

(127) I det andra scenariot när det gäller utbyte av uppgifter som samlats in av en brottsbekämpande myndighet med en underrättelsetjänst för ändamål som rör nationell säkerhet är den rättsliga grunden för sådant utbyte *Counter Terrorism Act 2008* ([208]). Enligt lagen om bekämpande av terrorism får var och en lämna information till vilken underrättelsetjänst som helst i syfte att fullgöra någon av dess funktioner, inbegripet ”nationell säkerhet”.

(128) När det gäller villkoren för utbyte av uppgifter för nationella säkerhetsändamål begränsar *Intelligence Services Act* och *Security Services Act* underrättelsetjänsternas möjligheter att inhämta uppgifter till vad som är nödvändigt för att de ska kunna fullgöra sina lagstadgade uppgifter. Behöriga myndigheter som omfattas av del 3 i dataskyddslagen från 2018 och som vill utbyta uppgifter med underrättelsetjänsterna kommer att behöva ta hänsyn till ett antal faktorer/begränsningar utöver de lagstadgade uppgifterna för de organ som anges i lagen om underrättelsetjänster och lagen om säkerhetstjänster ([209]). I avsnitt 20 i *Counter Terrorism Act 2008* klargörs att all datadelning enligt avsnitt 19 i *Counter Terrorism Act 2008* fortfarande måste vara förenlig med dataskyddslagstiftningen; Detta innebär att alla begränsningar och krav i dataskyddslagen från 2018 gäller. Dessutom är brottsbekämpande myndigheter och underrättelsetjänster offentliga myndigheter i den mening som avses i *Human Rights Act 1998* och måste därför se till att de agerar i enlighet med de rättigheter som garanteras i Europakonventionen, inbegripet artikel 8. Med ord innebär dessa krav att all datadelning mellan brottsbekämpande organ och underrättelsetjänster ska vara förenlig med dataskyddslagstiftningen och Europakonventionen.

(129) Underrättelsetjänsters behandling av personuppgifter som mottagits eller erhållits från brottsbekämpande myndigheter för ändamål som rör nationell säkerhet omfattas av ett antal villkor och skyddsåtgärder ([210]). Del 4 i dataskyddslagen från 2018 gäller all behandling som utförs av underrättelsetjänsterna eller för deras räkning. Där

([207]) Kommissionens genomförandebeslut i enlighet med Europaparlamentets och rådets direktiv (EU) 2016/679 om adekvat skydd av personuppgifter i Förenade kungariket C(2021)4800.

([208]) Avsnitt 19 i lagen om bekämpande av terrorism från 2008 finns på följande länk: https://www.legislation.gov.uk/ukpga/2008/28/section/19

([209]) I avsnitt 2.2 i *Intelligence Service Act 1994* (se https://www.legislation.gov.uk/ukpga/1994/13/contents) föreskrivs följande: ”Chefen för underrättelsetjänsten ska ansvara för dess effektivitet och det ska vara hans skyldighet att säkerställa a) att det finns arrangemang för att säkerställa att ingen information erhålls av underrättelsetjänsten utom i den mån det är nödvändigt för att den ska kunna utföra sina uppgifter på ett korrekt sätt och att inga uppgifter lämnas ut av den utom i den mån det är nödvändigt för detta ändamål, ii) av hänsyn till den nationella säkerheten, iii) i syfte att förebygga eller upptäcka allvarliga brott, eller iv) i samband med straffrättsliga förfaranden och b) att underrättelsetjänsten inte vidtar några åtgärder för att främja något av Förenade kungarikets politiska partiers intressen” medan det i avsnitt 2.2 i *Security Service Act 1989* (se https://www.legislation.gov.uk/ukpga/1989/5/contents) föreskrivs att ”generaldirektören ska ansvara för tjänstens effektivitet och det ska vara hans skyldighet att säkerställa a) att det finns arrangemang för att säkerställa att inga uppgifter erhålls av avdelningen utom i den mån det är nödvändigt för att den ska kunna utföra sina uppgifter på ett korrekt sätt eller om det inte är nödvändigt för detta ändamål eller för att förebygga eller upptäcka brott, b) att tjänsten inte vidtar några åtgärder för att främja något politiskt partis intressen, och c) att det finns arrangemang som överenskommits med *Director General för National Crime Agency* för att samordna myndighetens verksamhet i enlighet med avsnitt 1.4 i denna lag med polisens, National Crime Agency’s och andra brottsbekämpande organs verksamhet”.

([210]) Skyddsåtgärder och begränsningar av underrättelsetjänsternas befogenheter regleras också i 2016 års lag om utredningsbefogenheter som tillsammans med 2000 års lag om utredningsbefogenheter för England, Wales och Nordirland och 2000 års lag om utredningsbefogenheter (Skottland) för Skottland utgör den rättsliga grunden för användningen av sådana befogenheter. Dessa befogenheter är dock inte relevanta i samband med ”vidareutbyte” eftersom de omfattar direkt insamling av personuppgifter av underrättelsetjänster. För en bedömning av underrättelsetjänsternas befogenheter enligt lagen om utredningsbefogenheter, se kommissionens genomförandebeslut enligt Europaparlamentets och rådets förordning (EU) 2016/679 om adekvat skydd av personuppgifter i Förenade kungariket C (2021) 4800.

fastställs de viktigaste principerna för dataskydd (laglighet, rättvisa och öppenhet ([211]), ändamålsbegränsning ([212]), uppgiftsminimering ([213]), precision ([214]), lagringsbegränsningar ([215]) och säkerhet ([216]), villkor för behandling av särskilda kategorier av uppgifter ([217]), bestämmelser om registrerades rättigheter ([218]), krav på inbyggt dataskydd ([219]) och internationella överföringar av personuppgifter ([220]).

(130) Samtidigt föreskrivs i avsnitt 110 i dataskyddslagen från 2018 ett undantag från de specificerade bestämmelserna i del 4 i dataskyddslagen från 2018 när ett sådant undantag krävs för att skydda den nationella säkerheten. I avsnitt 110.2 i dataskyddslagen från 2018 förtecknas de bestämmelser från vilka undantag är tillåtna. Detta omfattar dataskyddsprinciperna (med undantag för legalitetsprincipen), den registrerades rättigheter, skyldigheten att informera *Information Commissioner* om ett personuppgiftsbrott, inspektionsbefogenheter för *Information Commissioner* i enlighet med internationella skyldigheter, vissa av verkställighetsbefogenheterna för *Information Commissioner*, bestämmelser som gör vissa dataskyddsbrott till lagbrott och bestämmelser om särskilda ändamål för behandling, till exempel journalistiska, akademiska eller konstnärliga ändamål. Detta undantag kan grundas på en analys från fall till fall ([221]). Enligt Förenade kungarikets myndigheters förklaring, som bekräftas av rättspraxis från domstolar i Förenade kungariket, måste den ”personuppgiftsansvariga a) beakta de faktiska konsekvenserna för den nationella säkerheten eller försvaret om de var tvungna att följa den särskilda dataskyddsbestämmelsen och om de rimligen kunde följa den vanliga regeln utan att påverka den nationella säkerheten eller det nationella försvaret” ([222]). Huruvida undantaget har använts på lämpligt sätt omfattas av den tillsyn som utövas av ICO ([223]).

([211]) Enligt avsnitt 86.6 i dataskyddslagen från 2018 ska den metod med vilken uppgifterna erhålls beaktas för att avgöra om behandlingen sker på ett rättvist och öppet sätt. I detta avseende uppfylls kravet på rättvisa och öppenhet om uppgifterna erhålls från en person som lagligen har tillstånd eller är skyldig att tillhandahålla dem.

([212]) Enligt avsnitt 87 i dataskyddslagen från 2018 ska ändamålen med behandlingen vara specifika, uttryckligt angivna och legitima. Uppgifterna får inte behandlas på ett sätt som är oförenligt med de ändamål för vilka de samlades in. Enligt avsnitt 87.3 får ytterligare kompatibel behandling av personuppgifter endast tillåtas om den personuppgiftsansvariga enligt lag är behörig att behandla uppgifterna för detta ändamål och behandlingen är nödvändig och står i proportion till det andra ändamålet. Behandlingen bör anses vara förenlig om behandlingen består av behandling för arkivändamål av allmänt intresse, för vetenskapliga eller historiska forskningsändamål eller för statistiska ändamål och är föremål för lämpliga skyddsåtgärder (avsnitt 87.4 i dataskyddslagen från 2018).

([213]) Personuppgifter måste vara adekvata, relevanta och inte överdrivet omfattande (avsnitt 88 i dataskyddslagen från 2018).

([214]) Personuppgifter måste vara korrekta och aktuella (avsnitt 89 i dataskyddslagen från 2018).

([215]) Personuppgifter får inte lagras längre än nödvändigt (avsnitt 90 i dataskyddslagen från 2018).

([216]) Den sjätte principen om dataskydd är att personuppgifter ska behandlas på ett sätt som inbegriper vidtagande av lämpliga säkerhetsåtgärder när det gäller risker i samband med behandling av personuppgifter. Riskerna omfattar (men är inte begränsade till) oavsiktlig eller obehörig åtkomst till eller förstörelse, förlust, användning, ändring eller utlämnande av personuppgifter (avsnitt 91 i dataskyddslagen från 2018). I avsnitt 107 föreskrivs också att 1) varje registeransvarig ska vidta lämpliga säkerhetsåtgärder som är lämpliga med hänsyn till de risker som uppstår i samband med behandlingen av personuppgifter och 2) vid automatiserad behandling ska varje registeransvarig och personuppgiftsbiträde vidta förebyggande eller begränsande åtgärder på grundval av en riskbedömning.

([217]) Avsnitt 86.2 b och tillägg 10 i dataskyddslagen från 2018.

([218]) Del 4 kapitel 3 i dataskyddslagen från 2018, särskilt när det gäller rättigheterna om tillgång, rättelse och radering, invända mot behandlingen och inte vara föremål för automatiserat beslutsfattande, att ingripa i automatiserat beslutsfattande och informeras om beslutsfattandet. Dessutom måste den personuppgiftsansvariga informera den registrerade om behandlingen av hans eller hennes personuppgifter.

([219]) Avsnitt 103 i dataskyddslagen från 2018.

([220]) Avsnitt 109 i dataskyddslagen från 2018. Överföring av personuppgifter till internationella organisationer eller länder utanför Förenade kungariket är möjlig om överföringen är en nödvändig och proportionell åtgärd som utförs inom ramen för den personuppgiftsansvarigas lagstadgade uppgifter eller för andra ändamål som anges i särskilda avsnitt i *Security Service Act 1989* och *Intelligence Services Act 1994*.

([221]) Se målet Baker/Secretary of State for the Home Department [2001] UKit NSA2 (”Baker mot Secretary of State”).

([222]) *UK Explanatory Framework for Adequacy Discussions, section H:* National Security Data Protection and Investigatory Powers Framework, s. 15–16. Finns på följande länk: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872239/H_-_National_Security.pdf. Se även domen i målet Baker/Secretary of State (se fotnot 220 ovan) där domstolen upphävde ett nationellt säkerhetsintyg som utfärdats av inrikesministern och bekräftade tillämpningen av undantaget för nationell säkerhet eftersom den ansåg att det inte fanns någon anledning att föreskriva ett generellt undantag från skyldigheten att besvara begäranden om tillgång och att ett sådant undantag under alla omständigheter utan en bedömning i varje enskilt fall överskred vad som var nödvändigt och proportionerligt för skyddet av den nationella säkerheten.

([223]) Se samförståndsavtalet mellan ICO och UKIC enligt vilket ”När ICO mottar ett klagomål från en registrerad kommer det att försäkra sig om att frågan har hanterats korrekt och, i förekommande fall, att eventuella undantag har tillämpats på lämpligt sätt” (*Memorandum of Understandings between Information Commissioner's Office and the UK Intelligence Community*, punkt 16, finns på följande länk: https://ico.org.uk/media/about-the-ico/mou/2617438/uk-intelligence-community-ico-mou.pdf).

(131) När det gäller möjligheten att begränsa någon av de ovannämnda rättigheterna till skydd av ”nationell säkerhet” förskrivs i avsnitt 79 i dataskyddslagen från 2018 att en personuppgiftsansvarig har möjlighet att ansöka om ett intyg som undertecknats av en minister eller Attorney General och intygar att en begränsning av sådana rättigheter är, eller har varit, en nödvändig och proportionell åtgärd för att skydda den nationella säkerheten ([224]). Förenade kungarikets regering har utfärdat riktlinjer om nationella säkerhetscertifikat enligt dataskyddslagen från 2018 där det särskilt framhålls att varje begränsning av registrerades rättigheter för att skydda den nationella säkerheten måste vara proportionerlig och nödvändig ([225]). Samtliga nationella säkerhetscertifikat måste offentliggöras på ICO:s webbplats ([226]).

(132) Intyget bör gälla för en bestämd period på högst fem år så att det regelbundet ses över av den verkställande makten ([227]). I ett certifikat ska det anges vilka personuppgifter eller kategorier av personuppgifter som omfattas av undantaget samt vilka bestämmelser i dataskyddslagen från 2018 som undantaget gäller ([228]).

(133) Det är viktigt att lägga märke till att de nationella säkerhetscertifikaten inte medger ytterligare skäl att begränsa rätten till dataskydd med hänvisning till den nationella säkerheten. Med andra ord kan den personuppgiftsansvariga eller personuppgiftsbiträdet endast förlita sig på ett certifikat när de har konstaterat att det är nödvändigt att tillämpa undantaget för nationell säkerhet, vilket måste ske från fall till fall. Även om ett nationellt säkerhetsintyg är tillämpligt på ärendet i fråga kan ICO undersöka om det var motiverat att åberopa undantaget för nationell säkerhet i ett visst fall ([229]).

(134) Varje person som direkt berörs av utfärdandet av intyget kan överklaga intyget till Upper Tribunal ([230]) eller ([231]), om certifikatet identifierar uppgifter genom en allmän beskrivning, bestrida tillämpningen av intyget på specifika uppgifter ([232]).

(135) Skiljedomstolen kommer att ompröva beslutet att utfärda ett certifikat och besluta om det fanns rimliga skäl att utfärda intyget ([233]). Den kan behandla ett stort antal frågor, bland annat nödvändighet, proportionalitet och laglighet, med beaktande av konsekvenserna för de registrerades rättigheter och avvägningen av behovet av att skydda den nationella säkerheten. Till följd av detta kan domstolen fastställa att intyget inte är tillämpligt på specifika personuppgifter som är föremål för överklagandet ([234]).

([224]) Genom dataskyddslagen från 2018 upphävdes möjligheten att utfärda certifikat enligt avsnitt 28.2 i dataskyddslagen från 1998. Möjligheten att utfärda ”gamla certifikat” finns emellertid fortfarande om det rör sig om ett bestridande enligt lagen från 1998 (se tillägg 20 del 5 punkt 17 i lagen om dataskydd från 2018). Emellertid är detta mycket sällan förekommande och kommer endast att gälla ett begränsat antal fall, exempelvis om den registrerade bestrider hur en offentlig myndighet har tillämpat undantaget för nationell säkerhet på uppgiftsbehandlingen enligt 1998 års lag. Det bör noteras att avsnitt 28 i dataskyddslagen från 1998 kommer att gälla i sin helhet i dessa fall, vilket därmed ger den registrerade möjlighet att bestrida certifikatet. För närvarande har inga nationella säkerhetscertifikat utfärdats enligt dataskyddslagen från 1998.

([225]) Förenade kungarikets regerings vägledning om nationella säkerhetscertifikat *(UK Government Guidance on National Security Certificates)* enligt dataskyddslagen från 2018, finns på följande länk: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf.

([226]) Enligt avsnitt 130 i dataskyddslagen från 2018, får ICO besluta att inte offentliggöra hela eller delar av certifikatets text, om det skulle strida mot den nationella säkerheten, strida mot allmänintresset eller äventyra en enskild persons säkerhet. I sådana fall skulle ICO emellertid offentliggöra det faktum att certfikatet har utfärdats.

([227]) Förenade kungarikets regerings vägledning om nationella säkerhetscertifikat, punkt 15 (se fotnot 225).

([228]) Förenade kungarikets regerings vägledning om nationella säkerhetscertifikat, punkt 5 (fotnot 225).

([229]) Enligt avsnitt 102 i dataskyddslagen från 2018 ska den personuppgiftsansvariga kunna visa att han eller hon har följt dataskyddslagen från 2018. Detta innebär att en underrättelsetjänst skulle behöva visa för ICO att den har beaktat de särskilda omständigheterna i fallet när den förlitar sig på undantaget. ICO publicerar också en förteckning över de nationella säkerhetscertifikaten, som finns på följande länk: https://ico.org.uk/about-the-ico/our-information/national-security-certificates/.

([230]) Upper Tribunal är den domstol som är behörig att pröva överklaganden av beslut som fattats av lägre förvaltningsdomstolar och har särskild behörighet att överklaga beslut från vissa statliga organ.

([231]) Avsnitt 111 (3) i dataskyddslagen från 2018.

([232]) Avsnitt 111.5 i dataskyddslagen från 2018.

([233]) I målet Baker/Secretary of State (se fotnot 221) upphävde informationsdomstolen ett intyg om nationell säkerhet som utfärdats av Home Secretary eftersom den ansåg att det inte fanns någon anledning att föreskriva ett generellt undantag från skyldigheten att besvara begäranden om tillgång och att ett sådant undantag under alla omständigheter utan en analys från fall till fall överskred vad som var nödvändigt och proportionerligt för att skydda den nationella säkerheten.

([234]) Förenade kungarikets regerings vägledning om nationella säkerhetscertifikat, punkt 25, fotnot 225.

(136) En annan uppsättning möjliga begränsningar gäller dem som enligt tillägg 11 till dataskyddslagen från 2018 är tillämpliga på vissa bestämmelser i del 4 i dataskyddslagen från 2018 ([235]) för att skydda andra viktiga mål av allmänt intresse eller skyddade intressen, till exempel parlamentariska privilegier, rätten till förtrolig kommunikation mellan advokat och klient, genomförandet av rättsliga förfaranden eller de väpnade styrkornas stridsförmåga. Tillämpningen av dessa bestämmelser är antingen undantagen för vissa kategorier av information ("typbaserad") eller undantagen i den mån tillämpningen av dessa bestämmelser sannolikt skulle skada det skyddade intresset ("skadebaserat") ([236]). Fördomsbaserade undantag kan endast åberopas i den mån tillämpningen av den angivna dataskyddsbestämmelsen sannolikt skulle skada det specifika intresset i fråga. Användning av ett undantag måste därför alltid motiveras med hänvisning till den relevanta skada som sannolikt skulle uppstå i det enskilda fallet. Klassbaserade undantag kan endast åberopas med avseende på den specifika, snävt definierade informationskategori för vilken undantaget beviljas. Dessa liknar varandra i syfte och verkan med flera av undantagen i den brittiska dataskyddsförordningen (enligt tillägg 2 (Schedule 2) i dataskyddslagen från 2018) som i sin tur återspeglar undantagen i artikel 23 i dataskyddsförordningen.

(137) Av ovanstående följer att tillämplig lagstiftning i Förenade kungariket omfattar begränsningar och villkor, som också har tolkas så av domstolarna och Information Commission, för att säkerställa att dessa undantag och begränsningar håller sig inom gränserna för vad som är nödvändigt och proportionerligt för att skydda den nationella säkerheten.

(138) Underrättelsetjänsternas behandling av personuppgifter enligt del 4 i dataskyddslagen från 2018 övervakas av *Information Commissioner* ([237]).

(139) De allmänna uppgifterna för *Information Commissioner* när det gäller underrättelsetjänsters behandling av personuppgifter enligt del 4 i dataskyddslagen från 2018 fastställs i tillägg 13 till dataskyddslagen från 2018. Uppgifterna omfattar, men är inte begränsade till, övervakning och efterlevnad av del 4 i dataskyddslagen från 2018, främjande av allmänhetens medvetenhet, rådgivning till parlamentet, regeringen och andra institutioner om lagstiftningsåtgärder och administrativa åtgärder, främjande av personuppgiftsansvarigas och personuppgiftsbiträdens medvetenhet om sina skyldigheter, tillhandahållande av information till registrerade om utövandet av den registrerades rättigheter samt genomförande av utredningar.

(140) *Commissioner* har, liksom för del 3 i dataskyddslagen från 2018, befogenhet att underrätta personuppgiftsansvariga om en påstådd överträdelse och utfärda varningar om att en behandling sannolikt kommer att strida mot reglerna och utfärda reprimander när överträdelsen bekräftas. Han eller hon kan också utfärda förelägganden om verkställighet och påföljder för överträdelser av vissa bestämmelser i lagen ([238]). Till skillnad från vad som gäller för andra delar av dataskyddslagen från 2018 kan dock inte kommissionsledamoten lämna ett bedömningsföreläggande till ett organ för nationell säkerhet ([239]).

(141) I avsnitt 110 i dataskyddslagen från 2018 föreskrivs dessutom ett undantag från användningen av vissa av befogenheterna för *Commissioner* när detta krävs för att skydda den nationella säkerheten. Detta inbegriper

([235]) Detta omfattar: i) del 4 av dataskyddsprinciperna, med undantag för kravet på att behandlingen ska vara laglig enligt den första principen och det faktum att behandlingen måste uppfylla ett av de relevanta villkor som anges i tilläggen 9 och 10, ii) de registrerades rättigheter, och iii) skyldigheterna att rapportera överträdelser till ICO.

([236]) Enligt *UK Explanatory Framework* är de undantag som är "typbaserade" följande: i) Information om tilldelning av statliga hedersbetygelser och värdigheter. ii) Yrkesmässiga privilegier. iii) Konfidentiella uppgifter om anställning, yrkesutbildning eller utbildning. iv) Skriftliga prov och betyg. De "skadebaserade" undantagen rör frågorna i) förebyggande eller avslöjande av brott, gripande och lagföring av gärningsmän, ii) parlamentariskt privilegium, iii) rättsliga förfaranden, iv) kronans väpnade styrkors stridsförmåga, v) Förenade kungarikets ekonomiska välstånd, vi) förhandlingar med den registrerade, vii) vetenskaplig eller historisk forskning eller statistiska ändamål och viii) arkivering i allmänhetens intresse. *UK Explanatory Framework for Adequacy Discussions, section H: National Security*, s. 13 (se fotnot 222).

([237]) Avsnitt 116 i dataskyddslagen från 2018.

([238]) Enligt avsnitt 149.2 i förening med avsnitt 155 i lagen om dataskydd från 2018 kan förelägganden om verkställighet och påföljder utfärdas till en registeransvarig eller registerförare i samband med överträdelser av kapitel 2 i del 4 i dataskyddsmyndigheten 2018 (principer för behandling), en bestämmelse i del 4 i dataskyddsmyndigheten 2018 som ger den registrerade rättigheter, ett krav på att anmäla ett personuppgiftsbrott till ombudsmannen enligt avsnitt 108 i dataskyddsmyndigheten 2018 och principerna för överföring av personuppgifter till tredjeländer, länder som inte omfattas av konventionen och internationella organisationer i avsnitt 109 i dataskyddsmyndighetens 2018. (För närmare uppgifter om verkställighets- och påföljdsförelägganden, se skälen (102)–(103)).

([239]) Enligt avsnitt 147.6 i dataskyddslagen från 2018 får Information Commissioner inte lämna ett bedömningsföreläggande till ett organ som anges i avsnitt 23.3 i *Freedom of Information Act 2000*. Detta inbegriper Security service (MI5), Secret Intelligence Service (MI6) och Government Communications Headquarter.

befogenheterna för *Commissioner* att utfärda (alla typer av) påföljdsförelägganden enligt dataskyddsmyndigheten (informations-, bedömnings-, verkställighets och påföljdsförelägganden), befogenhet att utföra inspektioner i enlighet med internationella skyldigheter, befogenheter för inresa och inspektion samt regler om brott ([240]). Såsom förklaras i skäl (136) kommer dessa undantag endast att gälla om det är nödvändigt och proportionellt och från fall till fall. Tillämpningen av dessa undantag kan prövas i domstol ([241]).

(142) ICO och Förenade kungarikets underrättelsetjänster har undertecknat ett samförståndsavtal ([242]) som fastställer en ram för samarbete i ett antal frågor, bland annat anmälningar om personuppgiftsbrott och hantering av klagomål från registrerade. I synnerhet föreskrivs det att ICO efter att ha mottagit ett klagomål ska bedöma huruvida något undantag från nationell säkerhet har åberopats på lämpligt sätt. Svar på frågor från ICO i samband med granskningen av enskilda klagomål måste, enligt Förenade kungarikets regerings vägledning om nationella säkerhetscertifikat enligt dataskyddslagen, lämnas inom 20 arbetsdagar med hjälp av lämpliga säkra kanaler om det rör sig om sekretessbelagd information. Från april 2018 till dags dato har ICO mottagit 21 klagomål från enskilda personer om underrättelsetjänsterna. Varje klagomål bedömdes och resultatet meddelades den registrerade ([243]).

(143) Dessutom utövar underrättelse-och säkerhetsutskottet (*Intelligence and Security Committee* (ISC)) parlamentarisk tillsyn över underrättelsetjänsternas databehandling. Denna kommitté har sin rättsliga grund i *Justice and Security Act 2013* (lagen om rättvisa och säkerhet, JSA 2013) ([244]). Genom lagen inrättas underrättelse- och säkerhetsutskottet som ett utskott i Förenade kungarikets parlament. Underrättelse- och säkerhetsutskottet består av ledamöter som tillhör någon av parlamentets kammare och utses av premiärministern efter samråd med oppositionsledaren ([245]). Underrättelse- och säkerhetsutskottet ska lämna en årlig rapport till parlamentet om fullgörandet av sina uppgifter och andra rapporter som den anser lämpliga ([246]).

(144) Sedan 2013 har underrättelse- och säkerhetsutskottet fått större befogenheter, bland annat tillsyn över säkerhetstjänsternas operativa verksamhet. Enligt avsnitt 2 i *Justice and Security Act 2013* har underrättelse- och säkerhetsutskottet till uppgift att övervaka de nationella säkerhetsorganens utgifter, administration, politik och verksamhet. I *Justice and Security Act 2013* anges att underrättelse- och säkerhetsutskottet kan genomföra utredningar i operativa

([240]) Följande bestämmelser kan undantas: Avsnitt 108 (meddelande till Commissioner om personuppgiftsbrott), avsnitt 119 (inspektion i enlighet med internationella förpliktelser). Avsnitten 142–154 och tillägg 15 (förelägganden och befogenheter för Commissioner för tillträde och inspektion). Avsnitten 170–173 (personuppgiftsbrott). Dessutom när det gäller underrättelsetjänsternas behandling i tillägg 13 (andra allmänna uppgifter för Commissioner), punkt 1 a och g samt punkt 2.

([241]) Se t.ex. mål Baker/Secretary of State for the Home Department (se fotnot 221)

([242]) Samförståndsavtal mellan ICO och Förenade kungarikets underrättelsegemenskap, se fotnot 231.

([243]) I sju av dessa fall rådde ICO klaganden att ta upp frågan med den personuppgiftsansvariga (detta är fallet när en person har tagit upp en fråga med ICO, men borde först ha tagit upp frågan med den personuppgiftsansvariga), i ett av dessa fall gav ICO allmänna råd till den personuppgiftsansvariga (detta används när den personuppgiftsansvariga inte förefaller ha brutit mot lagstiftningen, men en bättre rutiner skulle kunna bidra till att frågan inte tas upp hos ICO), och i de övriga 13 fallen var den personuppgiftsansvariga inte skyldig att agera (detta används när frågor som tas upp av personer inte omfattas av dataskyddslagen från 2018 eftersom de visserligen rör behandling av personuppgifter, men på grundval av den information som tillhandahållits förefaller den personuppgiftsansvariga inte ha brutit mot lagen).

([244]) Som Förenade kungarikets myndigheter förklarade utvidgade *Justice and Security Act* ansvarsområde för *Intelligence and Security Committee* till att omfatta en roll när det gäller att övervaka underrättelsegemenskapen utöver de tre myndigheterna och möjliggöra en retroaktiv översyn av myndigheternas operativa verksamhet i frågor av stort nationellt intresse.

([245]) Avsnitt 1 i JSA 2013. Ministrarna är inte berättigade till medlemskap. Ledamöterna innehar sin ställning i *Intelligence and Security Committee* under hela det parlament när de utsågs. De kan avlägsnas genom ett beslut av det parlament genom vilket de utsågs om de upphör att vara en parlamentsledamot eller blir minister. En ledamot kan också avgå.

([246]) Utskottets betänkanden och uttalanden finns på följande webbadress: http://isc.independent.gov.uk/committee-reports. År 2015 utfärdade *Intelligence and Security Committee* en rapport om integritet och säkerhet: A modern and transparent legal framework" (se: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312_ISC_P%2BS%2BRpt%28web%29.pdf), där den granskade den rättsliga ramen för de övervakningstekniker som används av underrättelsetjänsterna och utfärdade en rad rekommendationer som sedan övervägdes och integrerades i förslaget till lag om utredningsbefogenheter som omvandlades till lag, 2016 års lag om utredningsbefogenheter. Regeringens svar på rapporten om personlig integritet och säkerhet finns på följande länk: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20151208_Privacy_and_Security_Government_Response.pdf.

frågor som inte rör pågående insatser ([247]). I det samförståndsavtal som premiärministern och underrättelse- och säkerhetsutskottet ([248]) kommit överens om anges i detalj vilka faktorer som ska beaktas när man överväger om en verksamhet inte är en del av en pågående insats ([249]). underrättelse- och säkerhetsutskottet kan också uppmanas att utreda pågående insatser av premiärministern och kan granska information som tillhandahålls frivilligt av organen.

(145) Enligt tillägg 1 till JSA 2013 får underrättelse- och säkerhetsutskottet begära att cheferna för någon av de tre underrättelsetjänsterna lämnar ut vilken information som helst. Myndigheten ska göra sådan information tillgänglig, såvida inte ministern lägger in sitt veto mot den ([250]). Förenade kungarikets myndigheter förklarade att underrättelse- och säkerhetsutskottet i praktiken undanhålls mycket lite information ([251]).

(146) När det gäller gottgörelse enligt avsnitt 165.2 i dataskyddslagen från 2018 får en registrerad för det första lämna in ett klagomål till ICO om han eller hon anser att det föreligger en överträdelse av del 4 i dataskyddslagen från 2018 i samband med personuppgifter som rör honom eller henne, inbegripet missbruk av undantag och begränsningar för den nationella säkerheten.

(147) Enligt del 4 i dataskyddslagen från 2018 har enskilda dessutom rätt att ansöka hos High Court (eller Court of Session in Scotland) om ett föreläggande om att den personuppgiftsansvariga ska iaktta rätten till tillgång till uppgifter ([252]), invända mot behandling ([253]) och rättelse eller radering.

(148) Enskilda har också rätt att från den personuppgiftsansvariga eller personuppgiftsbiträdet begära ersättning för skada till följd av överträdelse av ett krav i del 4 i dataskyddslagen från 2018 ([254]). Med skada avses både ekonomisk förlust och skada som inte medför ekonomiska förluster, till exempel nödläge ([255]).

(149) Slutligen kan en enskild person lämna in ett klagomål till domstolen för utredningsbefogenheter (*Investigatory Powers Tribunal*) för alla handlingar som begåtts av eller på uppdrag av Förenade kungarikets underrättelsetjänster ([256]). Domstolen för utredningsbefogenheter (IPT) inrättades genom 2000 års lag om utredningsbefogenheter för England, Wales och Nordirland och 2000 års lag om utredningsbefogenheter (Skottland) för Skottland (RIPA 2000) och är oberoende av den verkställande makten ([257]). Enligt avsnitt 65 i 2000 års lag om utredningsbefogenheter utses Investigatory Powers Tribunals ledamöter av drottningen för en period på fem år.

(150) En ledamot av tribunalen kan avsättas från sitt ämbete av drottningen efter en framställning ([258]) i båda kamrarna i parlamentet ([259]).

(151) För att väcka talan vid Investigatory Powers Tribunal (”stående krav”), enligt avsnitt 65 i 2000 års lag om utredningsbefogenheter, måste en enskild tro i) att en underrättelsetjänst har agerat med avseende på honom eller henne, någon av hans eller hennes egendom, alla meddelanden som skickats av eller till honom eller som är avsedda för honom eller henne eller hans eller hennes användning av post-, telekommunikationstjänster eller telekommunikationssystem ([260]) och ii) att

([247]) Avsnitt 2 i JSA 2013.
([248]) Samförståndsavtal mellan premiärministern och *Intelligence and Security Committee*, finns på följande länk: http://data.parliament.uk/DepositedPapers/Files/DEP2013-0415/AnnexA-JSBill-summaryofISCMoU.pdf.
([249]) Samförståndsavtal mellan premiärministern och *Intelligence and Security Committee*, punkt 14 (se fotnot 248).
([250]) Ministern får endast lägga in veto mot utlämnande av uppgifter på följande två grunder: att uppgifterna är känsliga och inte bör lämnas ut till Intelligence and Security Committee med hänsyn till den nationella säkerheten, att om ministern anmodades att inkomma med den till ett av *Departmental Select Committee of the House of Commons*, skulle ministern (av skäl som inte är begränsade till den nationella säkerheten) anse att det var lämpligt att inte göra det (tillägg 1 punkt 4.2 i *Justice and Security Act 2013*).
([251]) *UK Explanatory Framework – section H:* National Security, s. 43.
([252]) Avsnitt 94.11 i dataskyddslagen från 2018.
([253]) Avsnitt 99.4 i dataskyddslagen från 2018.
([254]) Avsnitt 169 i dataskyddslagen från 2018, som tillåter anspråk från ”en person som lider skada på grund av överträdelse av ett krav i dataskyddslagstiftningen”.
([255]) Avsnitt 169 (5) i dataskyddslagen från 2018.
([256]) Se avsnitt 65.2 b i lagen om utredningsbefogenheter.
([257]) Enligt tillägg 3 till 2000 års lag om utredningsbefogenheter måste ledamöterna ha särskild erfarenhet inom rättsväsendet och kunna återutnämnas.
([258]) När det gäller begreppet ”adress” (se fotnot 183).
([259]) Tillägg 3 punkt 1.5 till 2000 års lag om utredningsbefogenheter.
([260]) Avsnitt 65.4 i 2000 års lag om utredningsbefogenheter.

beteendet har ägt rum under ”jäviga omständigheter” ([261]) eller ”utförts av underrättelsetjänsterna eller för deras räkning” ([262]). Eftersom denna ”övertygelse” i synnerhet har tolkats ganska brett ([263]), omfattas ett mål vid tribunalen av relativt låga krav på talerätt.

(152) När tribunalen prövar ett klagomål som lämnats till den är det tribunalens skyldighet att undersöka huruvida de personer som anklagas i klagomålet har varit inblandade i klagomålet samt att undersöka vilken myndighet som påstås ha begått överträdelserna och huruvida det påstådda beteendet har ägt rum ([264]). När tribunalen prövar ett mål ska den tillämpa samma principer för att avgöra målet som de som skulle tillämpas av en domstol vid en ansökan om rättslig prövning ([265]).

(153) Tribunalen ska underrätta klaganden om huruvida det har beslutats till hans eller hennes fördel eller inte ([266]). Enligt avsnitten 67.6 och 67.7 i 2000 års lag om utredningsbefogenheter är tribunalen behörig att besluta om interimistiska åtgärder och att meddela sådan ersättning eller andra föreläggande som den finner lämpliga ([267]). Enligt avsnitt 67A i 2000 års lag om utredningsbefogenheter kan ett avgörande från tribunalen överklagas med förbehåll för tribunalens eller den relevanta appellationsdomstolens tillstånd.

(154) I synnerhet kan enskilda personer väcka talan – och få gottgörelse – inför domstolen för utredningsbefogenheter om de anser att en offentlig myndighet har agerat (eller avser att agera) på ett sätt som är oförenligt med en av rättigheterna enligt den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna, inbegripet rätten till integritet och dataskydd och följaktligen är olaglig enligt avsnitt 6.1 i *Human Rights Act 1998*. Domstolen för utredningsbefogenheter som har beviljats exklusiv behörighet för alla anspråk enligt *Human Rights Act* i förhållande till underrättelsetjänsterna. Detta innebär, som High Court har påpekat, att ”huruvida det har förekommit ett brott mot *Human Rights Act* i ett enskilt fall är något som i princip kan tas upp och avgöras av en oberoende tribunal som kan få tillgång till allt relevant material, inbegripet hemligt material. […] Vi har också i detta sammanhang i åtanke att Investigatory Powers Tribunal nu är föremål för möjligheten att överklaga till en lämplig appellationsdomstol (i England och Wales, som skulle vara Court of Appeal) och att Supreme Court nyligen har beslutat att Investigatory Powers Tribunal i princip kan bli föremål för domstolsprövning, se R (Privacy International)/Investigatory Powers Tribunal [2019] UKSC 22, [2019] 2 WLR 1219” ([268]). Om Investigatory Powers Tribunal finner att en offentlig myndighets agerande är rättsstridigt kan Investigatory Powers Tribunal bevilja en sådan befrielse, ett sådant rättsmedel eller fatta ett sådant beslut inom ramen för sina befogenheter på det sätt som den anser vara skäligt och lämpligt ([269]).

([261]) Sådana omständigheter avser offentliga myndigheters agerande med myndighetsutövning (t.ex. ett beslut, ett tillstånd/ett föreläggande om förvärv av meddelanden osv.) eller om omständigheterna är sådana (oavsett om det finns en sådan myndighet eller inte) att det inte skulle ha varit lämpligt att beteendet ägde rum utan det eller åtminstone utan att vederbörlig hänsyn hade tagits till huruvida en sådan befogenhet borde ha sökts. Ett agerande som har godkänts av en Judicial Commissioner anses ha ägt rum under omständigheter mot vilka talan kan väckas (avsnitt 65 (7ZA) i 2000 års lag om utredningsbefogenheter) medan andra handlingar som äger rum med tillstånd av en person som innehar ett domarämbete inte anses ha ägt rum under omständigheter mot vilka talan kan väckas (avsnitten 65.7 och 8 i 2000 års lag om utredningsbefogenheter).

([262]) Enligt de uppgifter som lämnats av Förenade kungarikets myndigheter visar den låga tröskeln för att lämna in ett klagomål att det inte är ovanligt att tribunalen i sin undersökning fastställer att klaganden i själva verket aldrig varit föremål för en utredning av en offentlig myndighet. I den senaste statistiska rapporten anges att Investigatory Powers Tribunal under 2016 mottog 209 klagomål, att 52 % av dessa ansågs vara av okynneskaraktär eller förargelseväckande och att 25 % fick ett ”inget beslut”-resultat. Förenade kungarikets myndigheter förklarade att detta antingen innebär att ingen hemlig verksamhet/inga dolda befogenheter har använts i förhållande till klaganden eller att dold teknik användes och tribunalen fastställde att verksamheten var laglig. Dessutom uteslöts 11 % från jurisdiktion, drogs tillbaka eller var inte giltiga, 5 % uteslöts för sent, 7 % konstaterades vara till klagandens fördel. Statistical Report of the Investigatory Powers Tribunal 2016 finns på följande länk: https://www.ipt-uk.com/docs/IPT%20Statisical%20Report%202016.pdf.

([263]) Se målet Human Rights Watch/Secretary of State [2016] UKIPTrib15_165-CH. I detta mål fann *Investigatory Powers Tribunal*, med hänvisning till Europadomstolens rättspraxis, att det lämpliga testet för att anta att alla handlingar som omfattas av underavsnitt 68.5 i 2000 års lag om utredningsbefogenheter har utförts av någon av underrättelsetjänsterna eller på uppdrag av någon av underrättelsetjänsterna är huruvida det finns någon grund för en sådan övertygelse, inbegripet det faktum att en enskild person kan göra anspråk på att vara offer för en överträdelse som orsakats av enbart förekomsten av hemliga åtgärder eller lagstiftning som medger hemliga åtgärder endast om han eller hon kan visa att han eller hon är utsatt för en sådan risk (se Human Rights Watch/Secretary of State, punkt 41).

([264]) Avsnitt 67.3 i 2000 års lag om utredningsbefogenheter.

([265]) Avsnitt 67.2 i 2000 års lag om utredningsbefogenheter.

([266]) Avsnitt 68.4 i 2000 års lag om utredningsbefogenheter.

([267]) Detta kan inbegripa ett beslut om att alla register över uppgifter som innehas av en offentlig myndighet om en person ska förstöras.

([268]) High Court of Justice, Liberty, [2019] EWHC 2057 (Admin), punkt 170.

([269]) Avsnitt 8.1 i *Human Rights Act 1998*.

(155) Efter att ha uttömt nationella rättsmedel kan en enskild få upprättelse vid Europeiska domstolen för de mänskliga rättigheterna för kränkningar av de rättigheter som garanteras enligt den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna, inbegripet rätten till integritet och dataskydd.

(156) Av ovanstående följer att Förenade kungarikets straffrättsliga myndigheters utbyte av uppgifter som överförs enligt detta beslut med andra offentliga myndigheter, inbegripet underrättelsetjänster, omfattas av begränsningar och villkor som säkerställer att sådant vidare delning kommer att vara nödvändigt och proportionerligt och omfattas av särskilda dataskyddsgarantier enligt dataskyddslagen från 2018. Dessutom övervakas behandlingen av uppgifter av de berörda offentliga myndigheterna av oberoende organ och berörda personer har tillgång till effektiva rättsmedel.

3. **SLUTSATS**

(157) Kommissionen anser att del 3 i dataskyddslagen från 2018 säkerställer en skyddsnivå för personuppgifter som överförs i brottsbekämpningssyfte från behöriga myndigheter i unionen till behöriga myndigheter i Förenade kungariket, som i allt väsentligt är likvärdig med det skydd som garanteras genom direktiv (EU) 2016/680.

(158) Kommissionen anser dessutom att tillsynsmekanismerna och möjligheterna till prövning i Förenade kungarikets lagstiftning sammantaget gör det möjligt att identifiera och bestraffa överträdelser i praktiken och erbjuda den registrerade rättsmedel för att få tillgång till personuppgifter som rör honom eller henne och, i slutändan, rättelse eller radering av sådana uppgifter.

(159) På grundval av tillgänglig information om Förenade kungarikets rättsordning anser kommissionen slutligen att varje ingrepp i de grundläggande rättigheterna för de personer vars personuppgifter överförs från Europeiska unionen till Förenade kungariket av myndigheter i Förenade kungariket för ändamål av allmänt intresse, inbegripet i samband med delning av personuppgifter mellan brottsbekämpande myndigheter och andra offentliga myndigheter, till exempel nationella säkerhetsorgan, kommer att begränsas till vad som är absolut nödvändigt för att uppnå det legitima målet i fråga och att det finns ett effektivt rättsligt skydd mot sådana ingrepp.

(160) Det bör därför beslutas att Förenade kungariket säkerställer en adekvat skyddsnivå i den mening som avses i artikel 36.2 i direktiv (EU) 2016/680, tolkad mot bakgrund av stadgan om de grundläggande rättigheterna.

(161) Denna slutsats grundar sig på både Förenade kungarikets relevanta inhemska system och dess internationella åtaganden, särskilt anslutningen till den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna och hänvändelse till Europeiska domstolen för de mänskliga rättigheterna. Fortsatt efterlevnad av sådana internationella förpliktelser är därför ett särskilt viktigt inslag i den bedömning som ligger till grund för detta beslut.

4. **EFFEKTERNA AV DETTA BESLUT OCH DATASKYDDSMYNDIGHETERNAS ÅTGÄRDER**

(162) Medlemsstaterna och deras organ är skyldiga att vidta de åtgärder som är nödvändiga för att följa unionsinstitutionernas rättsakter, eftersom dessa antas vara lagenliga och följaktligen har rättsverkningar fram till dess att de löper ut, återkallas, ogiltigförklaras inom ramen för en talan om ogiltigförklaring eller förklaras ogiltiga till följd av en begäran om förhandsavgörande eller en invändning om rättsstridighet.

(163) Följaktligen är ett kommissionsbeslut om adekvat skyddsnivå som antagits i enlighet med artikel 36.3 i direktiv (EU) 2016/680 bindande för alla organ i medlemsstaterna till vilka det är riktat, inbegripet deras oberoende tillsynsmyndigheter. Under tillämpningsperioden för detta beslut får överföringar från en personuppgiftsansvarig eller ett personuppgiftsbiträde i unionen till personuppgiftsansvariga eller personuppgiftsbiträden i Förenade kungariket ske utan ytterligare tillstånd.

(164) Samtidigt ska det erinras om att enligt artikel 47.5 i direktiv (EU) 2016/680, och såsom domstolen förklarade i domen i Schrems-målet, ska den nationella lagstiftningen, när en nationell dataskyddsmyndighet frågar om huruvida ett kommissionsbeslut om adekvat skyddsnivå är förenligt med den enskildes grundläggande rätt till personlig integritet och skydd av personuppgifter, innehålla ett rättsmedel för att framställa dessa invändningar till en nationell domstol, som kan vara skyldig att begära ett förhandsavgörande från EU-domstolen ([270]).

([270]) *Schrems*-målet, punkt 65.

5. ÖVERVAKNING, TILLFÄLLIGT UPPHÄVANDE, UPPHÄVANDE ELLER ÄNDRING AV DETTA BESLUT

(165) Enligt artikel 36.4 i direktiv (EU) 2016/680 ska kommissionen fortlöpande övervaka relevant utveckling i Förenade kungariket efter antagandet av detta beslut för att bedöma om det fortfarande säkerställer en väsentligen likvärdig skyddsnivå. En sådan övervakning är särskilt viktig i detta fall, eftersom Förenade kungariket kommer att administrera, tillämpa och verkställa ett nytt system för skydd av personuppgifter som inte längre omfattas av unionsrätten, vilket kan komma att utvecklas. Särskild uppmärksamhet kommer att riktas mot hur Förenade kungarikets regler om överföring av personuppgifter till tredjeland tillämpas i praktiken, inbegripet genom internationella avtal, och hur tillämpningen påverkar den skyddsnivå som ges uppgifter som överförs enligt detta beslut. Dessutom kommer kommissionen att vara uppmärksam på om individuella rättigheter kan utövas på ett effektivt sätt på de områden som omfattas av detta beslut. Kommissionens övervakning kommer bland annat att baseras på utvecklingen av rättspraxis och den tillsyn som utförs av ICO och andra oberoende organ.

(166) För att underlätta denna övervakning bör Förenade kungarikets myndigheter omgående och regelbundet informera kommissionen om alla väsentliga ändringar av Förenade kungarikets rättsordning som påverkar den rättsliga ram som är föremål för detta beslut, liksom om eventuella förändringar av praxis i samband med den behandling av personuppgifter som bedöms i detta beslut, i synnerhet i fråga om sådant som nämns i skäl(165).

(167) För att kommissionen ska kunna utföra sin övervakningsfunktion på ett effektivt sätt bör medlemsstaterna dessutom informera kommissionen om alla relevanta åtgärder som vidtas av de nationella dataskyddsmyndigheterna, särskilt när det gäller förfrågningar eller klagomål från registrerade i EU om överföring av personuppgifter från unionen till behöriga myndigheter i Förenade kungariket. Kommissionen bör också informeras om eventuella indikationer på att de åtgärder som vidtas av Förenade kungarikets offentliga myndigheter med ansvar för att förebygga, utreda, avslöja eller lagföra brott, inbegripet eventuella tillsynsorgan, inte säkerställer den skyddsnivå som krävs.

(168) Om tillgänglig information, särskilt information från övervakningen av detta beslut eller från Förenade kungarikets eller medlemsstaternas myndigheter, visar att den skyddsnivå som Förenade kungariket erbjuder kanske inte längre är adekvat, bör kommissionen omgående informera de behöriga myndigheterna i Förenade kungariket om detta och begära att lämpliga åtgärder vidtas inom en angiven tidsram, som inte får överskrida tre månader. Med hänsyn tagen till problemets art och/eller de åtgärder som krävs får denna period vid behov förlängas med en angiven tidsperiod.

(169) Om de behöriga brittiska myndigheterna vid utgången av den angivna tidsfristen underlåter att vidta dessa åtgärder eller på annat tillfredsställande sätt visar att detta beslut fortfarande bygger på en adekvat skyddsnivå, kommer kommissionen att inleda det förfarande som avses i artikel 58.2 i direktiv (EU) 2016/680 i syfte att helt eller delvis tillfälligt upphäva eller upphäva detta beslut.

(170) Alternativt kommer kommissionen att inleda detta förfarande i syfte att ändra beslutet, särskilt genom att underställa överföringar av uppgifter ytterligare villkor eller genom att begränsa räckvidden för konstaterandet om adekvat skyddsnivå endast till uppgiftsöverföringar för vilka en adekvat skyddsnivå fortfarande säkerställs.

(171) Vid vederbörligen motiverade och tvingande skäl till skyndsamhet kommer kommissionen att utnyttja möjligheten att i enlighet med det förfarande som avses i artikel 58.3 i direktiv (EU) 2016/680 anta genomförandeakter med omedelbar verkan som tillfälligt upphäver, upphäver eller ändrar beslutet.

6. GILTIGHETSTID OCH FÖRLÄNGNING AV DETTA BESLUT

(172) Det bör beaktas att Förenade kungariket, i slutet av den övergångsperiod som föreskrivs i utträdesavtalet och så snart övergångsbestämmelsen i artikel 782 i handels- och samarbetsavtalet mellan EU och Förenade kungariket upphör att gälla, kommer att administrera, tillämpa och verkställa ett nytt system för dataskydd jämfört med det system som gällde när landet var bundet av unionsrätten. Detta kan särskilt omfatta ändringar eller ändringar av ramen för dataskydd som bedöms i detta beslut, liksom annan relevant utveckling.

(173) Det är därför lämpligt att föreskriva att detta beslut ska tillämpas under en period av fyra år från och med dess ikraftträdande.

(174) Om framför allt information från övervakningen av detta beslut visar att slutsatserna om den skyddsnivå som säkerställs i Förenade kungariket fortfarande är sakligt och rättsligt motiverade, bör kommissionen senast sex månader innan detta beslut upphör att gälla inleda förfarandet för att ändra detta beslut genom att i princip förlänga dess tidsmässiga tillämpningsområde med ytterligare fyra år. Varje sådan genomförandeakt om ändring av detta beslut ska antas i enlighet med det förfarande som avses i artikel 58.2 i direktiv (EU) 2016/680.

7. **SLUTLIGA ÖVERVÄGANDEN**

(175) Europeiska dataskyddsstyrelsen offentliggjorde sitt yttrande ([271]), vilket har beaktats vid utarbetandet av detta beslut.

(176) De åtgärder som föreskrivs i detta beslut är förenliga med yttrandet från den kommitté som inrättats genom artikel 58 i direktiv (EU) 2016/680.

(177) I enlighet med artikel 6a i protokoll nr 21 om Förenade kungarikets och Irlands ställning med avseende på området med frihet, säkerhet och rättvisa, fogat till EU-fördraget och EUF-fördraget, är Irland inte bundet av bestämmelserna i direktiv (EU) 2016/680, och därmed inte heller detta genomförandebeslut, som rör medlemsstaternas behandling av personuppgifter när de bedriver verksamhet som omfattas av tredje delen avdelning V kapitel 4 eller kapitel 5 i EUF-fördraget, där Irland inte är bundet av bestämmelserna om de former av polissamarbete som föreskrivs i artikel 16 i EUF-fördraget. Enligt rådets genomförandebeslut (EU) 2020/1745 ([272]) ska direktiv (EU) 2016/680 dessutom börja tillämpas provisoriskt i Irland från och med den 1 januari 2021. Irland är därför bundet av detta genomförandebeslut, på samma villkor som gäller för tillämpningen av direktiv (EU) 2016/680 i Irland enligt genomförandebeslut (EU) 2020/1745 vad gäller det regelverk som landet deltar i.

(178) I enlighet med artiklarna 2 och 2a i protokoll nr 22 om Danmarks ställning, fogat till fördraget om Europeiska unionen och fördraget om Europeiska unionens funktionssätt, är Danmark inte bundet av bestämmelserna i direktiv (EU) 2016/680, och därmed inte heller av detta genomförandebeslut, och omfattas inte heller av deras tillämpning som rör medlemsstaternas behandling av personuppgifter när de utför verksamhet som omfattas av tredje delen avdelning V kapitel 4 eller kapitel 5 i EUF-fördraget. Eftersom direktiv (EU) 2016/680 är en utveckling av Schengenregelverket meddelade Danmark emellertid den 26 oktober 2016 sitt beslut att genomföra direktiv (EU) 2016/680 i enlighet med artikel 4 i det protokollet. Danmark är därför enligt internationell rätt skyldigt att genomföra detta genomförandebeslut.

(179) När det gäller Island och Norge utgör detta genomförandebeslut en utveckling av bestämmelserna i Schengenregelverket i enlighet med avtalet mellan Europeiska unionens råd och Republiken Island och Konungariket Norge om dessa båda staters associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket ([273]).

(180) När det gäller Schweiz utgör detta genomförandebeslut en utveckling av bestämmelserna i Schengenregelverket i enlighet med avtalet mellan Europeiska unionen, Europeiska gemenskapen och Schweiziska edsförbundet om Schweiziska edsförbundets associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket ([274]).

(181) När det gäller Liechtenstein utgör detta genomförandebeslut en utveckling av bestämmelserna i Schengenregelverket i enlighet med protokollet mellan Europeiska unionen, Europeiska gemenskapen, Schweiziska edsförbundet och Furstendömet Liechtenstein om Furstendömet Liechtensteins anslutning till avtalet mellan Europeiska unionen, Europeiska gemenskapen och Schweiziska edsförbundet om Schweiziska edsförbundets associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket ([275]).

([271]) *Opinion 15/2021 regarding the European Commission draft implementing decision pursuant to Directive (EU) 2016/680 on the adequate protection of personal data in the United Kingdom*, finns på följande länk:https://edpb.europa.eu/our-work-tools/our-documents/opinion-led/opinion-152021-regarding-european-commission-draft_en.

([272]) Rådets genomförandebeslut (EU) 2020/1745 av den 18 november 2020 om inledande av tillämpningen av bestämmelserna i Schengenregelverket om dataskydd och om provisoriskt inledande av tillämpningen av vissa bestämmelser i Schengenregelverket i Irland (EUT L 393, 23.11.2020, s. 3).

([273]) EUT L 176, 10.7.1999, s. 36.

([274]) EUT L 53, 27.2.2008, s. 52.

([275]) EUT L 160, 18.6.2011, s. 21.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Vid tillämpningen av artikel 36 i direktiv (EU) 2016/680 säkerställer Förenade kungariket en adekvat skyddsnivå för personuppgifter som överförs från Europeiska unionen till myndigheter i Förenade kungariket som ansvarar för att förebygga, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder.

Artikel 2

Närhelst de behöriga tillsynsmyndigheterna i medlemsstaterna, i syfte att skydda enskilda med avseende på behandlingen av deras personuppgifter, utövar sina befogenheter enligt artikel 47 i direktiv (EU) 2016/680 med avseende på överföringar av uppgifter till offentliga myndigheter i Förenade kungariket inom det tillämpningsområde som anges i artikel 1, ska den berörda medlemsstaten utan dröjsmål underrätta kommissionen om detta.

Artikel 3

1. Kommissionen ska fortlöpande övervaka tillämpningen av den rättsliga ram som ligger till grund för detta beslut, inbegripet villkoren för vidare överföring och utövande av individuella rättigheter, i syfte att bedöma om Förenade kungariket fortsätter att säkerställa en adekvat skyddsnivå i den mening som avses i artikel 1.

2. Medlemsstaterna och kommissionen ska underrätta varandra om fall där *Information Commissioner* eller någon annan behörig myndighet i Förenade kungariket underlåter att säkerställa att den rättsliga ram som ligger till grund för detta beslut efterlevs.

3. Medlemsstaterna och kommissionen ska underrätta varandra om alla indikationer på att Förenade kungarikets offentliga myndigheter ingriper i enskildas rätt till skydd av sina personuppgifter utöver vad som är absolut nödvändigt eller att det inte finns något effektivt rättsligt skydd mot sådana ingrepp.

4. Om kommissionen har indikationer på att en adekvat skyddsnivå inte längre säkerställs ska kommissionen underrätta de behöriga myndigheterna i Förenade kungariket och får tillfälligt upphäva, upphäva eller ändra detta beslut.

5. Kommissionen får tillfälligt upphäva, upphäva eller ändra detta beslut om bristande samarbete från Förenade kungarikets regerings sida hindrar kommissionen från att avgöra om konstaterandet i artikel 1 påverkas.

Artikel 4

Detta beslut ska upphöra att gälla den 27 juni 2025, såvida det inte förlängs i enlighet med det förfarande som avses i artikel 58.2 i direktiv (EU) 2016/680.

Artikel 5

Detta beslut riktar sig till medlemsstaterna.

Utfärdat i Bryssel den 28 juni 2021.

På kommissionens vägnar
Didier REYNDERS
Ledamot av kommissionen